Bidang Ilmu: Hukum

LAPORAN AKHIR

PENELITIAN DOSEN PEMULA

Pengiriman E-Mail Spam
sebagai Kejahatan Siber di Indonesia

Pengusul :

Eka Nugraha Putra, SH., MH.

NIDN : 0721108602

UNIVERSITAS MERDEKA MALANG

April 2016

HALAMAN PENGESAHAN

Judul Penelitian	:	**Pengiriman E-Mail Spam sebagai Kejahatan Siber di Indonesia**
Bidang Ilmu	:	Ilmu Hukum
Ketua Peneliti		
a. Nama Lengkap	:	Eka Nugraha Putra SH., MH.
b. NIP/NIK	:	858/FH
c. NIDN	:	0721108602
d. Pangkat/golongan	:	
e. Jabatan Fungsional	:	
f. Fakultas/jurusan	:	Hukum / Ilmu Hukum
g. Pusat Penelitian	:	LPPM Universitas Merdeka Malang
h. Alamat Instansi	:	Jl. Terusan Raya Dieng 62-64 Malang
i. Telp/Fax/E-mail	:	(0341) 568395/ Fax. (0341) 564994
Biaya yang diusulkan	:	Rp. 5.000.000 (Lima Juta Rupiah)

Malang, April 2016

Mengetahui,

Dekan Fakultas Hukum

Dr. H. Setiyono, S.H., M.H.
NIK : 358/FH

Peneliti,

Eka Nugraha Putra SH., MH.
NIK : 858/FH

Menyetujui,

Ketua Lembaga Penelitian,

Prof. Ir. Agus Suprapto Msc., PhD.
NIK : 312/FT

RINGKASAN

Internet merupakan bagian dari perkembangan teknologi, dimana internet memberikan banyak dampak, baik positif maupun negatif. 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. Dari segi perbuatannya, pengiriman e-mail spam ini cukup banyak merugikan, bahkan melanggar privasi. Beberapa negara juga telah mengaturnya sebagai salah satu jenis kejahatan siber (*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 siber. 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, Privasi, Kejahatan Siber*

PRAKATA

Penulis mengucapkan puji syukur kepada Tuhan Yang Maha Esa, atas selesainya laporan penelitian dengan judul "**Pengiriman E-mail Spam sebagai Kejahatan Siber**" dengan baik. Laporan akhir penelitian ini berisi hasil dan pembahasan dari penelitian kami selama mengerjakan penelitian.

Penulis mengucapkan banyak terima kasih atas semua pihak yang telah membantu penulis sehingga penelitian ini selesai dan dapat penulis tuangkan dalam bentuk laporan akhir penelitian ini.

Penulis berharap semoga hasil penelitian ini dapat bermanfaat bagi khazanah ilmu hukum, khususnya hukum pidana di Indonesia.

April 2016

Penulis

DAFTAR ISI

Halaman Pengesahan ii

Ringkasan iii

Prakata iv

Daftar Isi v

Daftar Bagan vii

Daftar Tabel viii

BAB 1 PENDAHULUAN

1.1. Latar Belakang Permasalahan 1

1.2. Pertanyaan Penelitian 3

1.3. Urgensi Penelitian Dilakukan 3

1.4. Luaran Penelitian 3

BAB 2 TINJAUAN PUSTAKA

2.1. Konsep dan Pengertian E-mail Spam 4

2.2. E-mail Spam dan Aspek Hukum Privasi di Internet 6

2.3. Konsep dan Pengertian Kejahatan Siber 8

2.4. Pelanggaran Privasi sebagai Kejahatan Siber 11

BAB 3 TUJUAN DAN MANFAAT PENELITIAN

3.1. Tujuan Penelitian 16

3.2. Manfaat Penelitian 16

BAB 4 METODE PENELITIAN

4.1. Pendekatan Penelitian 17

4.2. Jenis dan Sumber Data 17

4.3. Teknik Pengumpulan Data 17

4.4. Teknik Analisa Data 18

BAB 5 HASIL DAN PEMBAHASAN

5.1. E-mail Spam Didefinisikan sebagai Kejahatan Siber 19

5.2. Pengaturan Pelanggaran Privasi melalui E-Mail Spam dalam Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 21

5.3. Pengaturan Ideal Terkait E-Mail Spam sebagai Kejahatan Siber untuk Perlindungan Privasi dalam Hukum Pidana Indonesia 26

BAB 6 KESIMPULAN DAN SARAN

6.1. Kesimpulan 31

6.2. Saran 31

Daftar Pustaka 32

Biodata Peneliti

DAFTAR BAGAN

Bagan Hubungan Cyberspace, Cybercrime dan Cyberlaw 9

DAFTAR TABEL

Permasalahan yang Ditimbulkan oleh Spam 28

BAB 1
PENDAHULUAN

1.1. Latar Belakang Permasalahan

Internet telah membawa dampak perubahan yang sangat besar bagi masyarakat. Dimana segala kegiatan manusia telah dapat 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.

Sebagaimana halnya dengan perkembangan teknologi lainnya, internet dalam pemanfaatannya juga memberikan dampak baik secara positif maupun negatif. Sebagai sarana komunikasi, internet memberikan kemudahan bagi masyarakat karena kemudahan dan kecepatannya dalam bertukar dan menyebarkan informasi. Apabila dulu berkomunikasi menggunakan surat atau telepon, masyarakat kini dimudahkan oleh internet dengan keberadaan e-mail (electronic mail) atau surat elektronik.

Pemanfaatan e-mail sebagai kemudahan yang diberikan internet ini pun berpeluang menjadi sebuah 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.[1] Pada pengiriman e-mail spam dalam jumlah banyak, tentu menimbulkan ketidaknyamanan 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.[2]

Pada dasarnya internet merupakan dunia yang berbeda dengan 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*.

---

[1] Tanpa Penulis, Tanpa Tahun, *Spam*, www.techterms.com diakses pada 3 Maret 2015.
[2] Riyandi Andesma, 2013, *Wah Indonesia Masuk 10 Besar Negara Penghasil Spam*, www.techno.okezone.com diakses pada 3 Maret 2015.

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 asepk-aspek hukum terkait internet baik perdata maupun pidana. Dalam 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 mengenai 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 bahwa setiap pribadi di internet juga memiliki hak untuk tidak diganggu.

Apabila kembali kepada UU ITE pengaturan privasi sendiri di Pasal 26 kurang komperehensif 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 tersebut.

Berdasarkan uraian latar belakang di atas, maka Penulis mengangkat tema penelitian mengenai spam dan *cybercrime* dalam judul penelitian "**Pengiriman E-mail Spam sebagai Kejahatan Siber di Indonesia**".

1.2. Pertanyaan Penelitian

Meskipun di beberapa negara e-mail spam telah diklasifikan dalam kejahatan siber, Namun di Indonesia belum diatur dalam peraturan perundang-undangan terkait, dengan melihat latar belakang di atas serta pentingnya fokus penelitian mengenai spam dan kejahatan siber, maka Penulis mengangkat beberapa pertanyaan penelitian sebagai berikut :

1. Apakah e-mail spam dapat didefinisikan sebagai kejahatan siber ?
2. Bagaimana UU ITE mengatur mengenai privasi yang diganggu oleh e-mail spam ?
3. Bagaimana sebaiknya pengaturan e-mail spam dalam kaitannya dengan perlindungan privasi pada hukum pidana siber Indonesia ?

1.3. Urgensi Penelitian Dilakukan

Permasalahan yang diangkat dalam penelitian ini adalah permasalahan hukum yang bersifat baru dikarenakan berkaitan dengan perkembangan teknologi informasi. Dalam hal aspek hukum terkait privasi belum ada pengaturan secara spesifik dan lebih tegas. Tidak adanya pengaturan mengenai apa itu e-mail spam dan sanksi yang diberlakukan terhadap perbuatan pengiriman e-mail spam menciptakan permasalahn hukum baru dalam hukum pidana indonesia.

Hasil penelitian ini diharapkan dapat memberikan sumbangsih terhadap diskursus mengenai aspek hukum dalam privasi di internet serta membantu penegak hukum melegitimasi perbuatan pengiriman e-mail spam sebagai sebuah kejahatan siber.

1.4. Luaran Penelitian

Luaran dari penelitian ini adalah publikasi ilmiah dalam Jurnal Cakrawala Hukum Fakultas Hukum Universitas Merdeka Malang dan sebagai pengayaan bahan ajar mata kuliah Hukum Telematika.

BAB 2

TINJAUAN PUSTAKA

2.1. Konsep dan Pengertian E-Mail Spam

Penggunaan e-mail (*electronic mail*) atau dalam bahasa Indonesia digunakan terminologi surat elektronik, semakin jamak di kalangan masyarakat terutama sejak kehadiran internet. Kehadiran e-mail sebagai sarana berkomunikasi menggantikan surat dan telegram yang sudah banyak ditinggalkan. Penggunaannya yang praktis, mudah bahkan gratis menyebabkan e-mail merupakan salah satu fitur utama yang banyak digunakan saat ini.

E-mail tidak hanya bisa digunakan berkirim pesan selayaknya surat berbentuk fisik, namun dapat juga dilampirkan berbagai informasil elektronik atau file baik berbentuk tulisan, gambar, audio atau video meskipun dengan kapasitas yang terbatas. Sebagai contoh provider Gmail hanya memberikan 20 Megabyte sebagai batas maksimum pelampiran (*attachment*) *file* setiap emailnya.

Pada perkembangannya saat ini, e-mail banyak digunakan sebagai alat untuk memverifikasi data pengguna internet ketika hendak masuk ke dalam website atau akun jejaring sosial tertentu, seperti Facebook, Twitter, Path dan lain-lain.

Pada dasarnya berbagi dan bertukar informasi via e-mail memang sangat mudah dan bermanfaat, namun terdapat pula bentuk penyebaran dan pengiriman informasi yang bersifat mengganggu yang dinamakan dengan e-mail spam. Sama seperti pada teknologi SMS (*Short Messaging Service*) yang belakangan juga banyak mendapatkan spam. E-mail pun juga banyak tingkat pengiriman spamnya.

Spam pada dasarnya adalah perbuatan menyebar pesan yang dikirimkan secara bertubi-tubi.[3] Namun, berbeda dengan yang ada pada SMS, spam pada e-mail tidak hanya sekedar pengiriman pesan elektronik secara bertubi-tubi tetapi juga pengiriman pesan berbentuk informasi yang tidak penting atau bahkan tidak relevan. Informasi yang semacam ini, tak jarang pula juga berisikan informasi yang bertujuan untuk menipu penerima e-mail spam tersebut.

Sistem pengelolaan informasi pada e-mail sebenarnya bekerja dalam bentuk komunikasi satu pada satu (*one on one communication*), namun pada level ISP atau *Internet Service Provider* (ISP) e-mail berada pada tingkat penyebaran yang cukup tinggi. Pada level ISP penyebaran tidak hanya pada bentuk satu pada satu, namun juga banyak pada satu (*many*

[3] Christian Adhi Nugroho S, 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.

to one communication) atau juga dikenal dengan forwarded e-mail, serta *mailing lists* (*one to many communication*).[4]

Pada SMTP (*System Mail Transfer Protocol*), sebagai sistem pengelola seluruh e-mail di internet. SMTP ini didesain untuk menangkap informasi pada rute dimana informasi itu dikirim dari pengirim kepada penerima informasi, sehingga secara tidak langsung SMTP ini tidaklah memiliki perlindungan keamanan, karena tidak adanya privasi, rute yang bisa diubah dan sulitnya melacak sumber informasi. Kurangnya tingkat keamanan pada SMTP inilah yang seringkali dijadikan celah oleh pengirim e-mail spam untuk menyebarkan informasi yang tidak relevan atau bahkan pemalsuan dan penipuan.[5]

Pada dasarnya spam bisa terjadi dalam beragam bentuk : informasi menganggu yang berbentuk iklan secara halus, informasi yang menjadi titik masuk bagi kejahatan siber seperti pemalsuan data, penipuan atau pencurian data.[6] 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.

Pada ciri yang kedua memang biasanya terjadi pada pengguna internet yang tidak memahami tentang etika menggunakan internet. Hal ini lazim terjadi pada pengguna jejaring sosial, dimana terdapat pandangan yang menganggap bahwa internet adalah dunia yang bebas apalagi ketika internet memungkinkan penggunanya untuk menggunakan identitas anonim atau pseudonim. Sebagai contoh adalah tag pada Facebook dari pemiliki akun Facebook yang melakukan jual beli via Facebook. Hal ini sebenarnya juga merupakan bentuk spamming karena *tag* foto barang yang dilakukan belum tentu sesuai dengan minat pemilik akun Facebook yang di-*tag*, sehingga notifikasi yang muncul berkali-kali tentu saja menganggu.

Pada 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-

[4] Richard Clayton, 2007, *Email Traffic : A Quantitative Snapshot*, Makalah dipresentasikan pada Fourth Conference on Email and Anti Spam 2-3 Agustus 2007, Mountain View California, hal 1.
[5] Dan Boneh, 2004, *The Difficulities of Tracing Spam Email*, www.ftc.gov diakses pada 27 Februari 2015.
[6] Mamoun Alazab dan Roderic Broadhurst, 2015, *Spam and Criminal Activity*,*Trends and Issues (Australian Institute of Criminology) 2015 RegNet Research Paper No. 2014/44* hal 2.

kode rumit yang tidak jelas dipahami oleh penerima e-mailnya. Pengiriman e-mail spam ini juga dikirim dalam periode yang singkat namun dilakukan dengan nama pengirim, nama lampiran *file* (*attachment*) atau URL yang berbeda-beda. [7]

2.2. E-mail Spam dan Aspek Hukum Privasi di Internet

Bentuk pengiriman e-mail spam di atas memang memberikan gangguan, meskipun tidak semua pengiriman e-mail spam berisi *phising* (penyebaran virus atau malware) namun bagi penerima e-mail spam, jelas terdapat gangguan terhadap pribadi atau jaminan atas privasinya. Oleh karena itu, tentu perlu dipahami makna dan ruang lingkup privasi di Internet.

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 yaitu[8] :

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.

---

[7] *Ibid*.

[8] Sinta Dewi Rosadi, 2015, *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, Refika Aditama, Bandung, hal 20.

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.[9] Terdapat pandangan tradisional bahwa masalah privasi terlepas dari struktur hukum, sehingga privasi secara alamiah terancam oleh cepatanya perkembangan teknologi, di sinilah kemudian seharusnya hukum mengintervensi pengaturan privasi.[10] 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 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.[11]

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.[12]

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.[13]

---

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

[10] Daniel J. Solove, 2003, *Identity Theft, Privacy, and The Architecture of Vulnerability*, Hastings Law Journal Vol. 54, hal 14.

[11] Arthur Cockfield dan Jason Pridmore, 2007, *A Synthetic Theory of Law and Technology*, Minnersota Journal of Law, Science and Technology Vol 8 Number 2 Queens University, hal 483.

[12] Graham Greenleaf, 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, hal 2.

[13] Pasal 1 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*.

Berlaku sejak tahun 1998, Directive ini mengatur subjek *data, controller, processor, third party, recipient, supervisory authorities* sebagai pihak-pihak yang terlibat di dalam proses pengolahan data pribadi. Lahirnya Directive ini pula mendorong banyak negara-negara, khususnya Uni Eropa untuk membuat undang-undang terkait privasi dan perlindungan data pribadi atau merevisi undang-undang yang sudah ada.

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. Undang-Undsang Nomor 43 Tahun 2009 Tentang Kearsipan yang mengatur dan membedakan arsip dinamis dan arsip vital[14], Undang-Undang Nomor 36 Tahun 1999 Tentang HAM yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya[15], Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan dimana bank diwajibkan untuk merahasiakan keterangan tentang nasabah penyimpan dan simpanannya, kecuali untung kepentingan perpajakan, penyelesaian piutang bank, kepentingan peradilan dan perkara pidana[16], Undang-Undang Nomor Kesehatan, 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.[17]

Berkaitan dengan perlindungan data pribadi di internet dan privasi di internet terdapat UU ITE dimana pengaturannya akan dibahas lebih jauh pada bab V penelitian ini.

2.3. Konsep dan Pengertian Kejahatan Siber

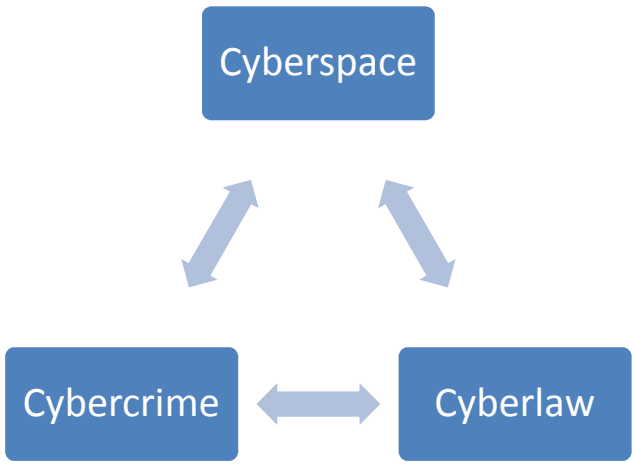
Internet tidak bisa dipungkiri telah melahirkan dunia yang baru, internet sebagai bagian dari konvergensi telematika (telekomunikasi, media dan informatika) menandai datangnya era baru di dunia dimana masyarakat melakukan aktivitasnya melalui jaringan komputer. Keberadaan teknologi, khususnya internet tentu tidak tepat bila hanya diatur oleh norma etika saja, namun diperlukan juga norma hukum yang mampu mengaturnya sehingga kemudian lahirlah hukum siber (*cyberlaw*).

Penggunaan istilah hukum siber sendiri lahir dari kata *cybernetics*, dimana *cybernetics* merupakan ilmu pengetahuan tentang mengatur atau mengarahkan sistem mulai dari yang paling sederhana hingga yang paling kompleks dengan cara memahami sistem dan

[14] Pasal 1 Angka 3 dan Angka 4 Undang-Undang Nomor 43 Tahun 2009 Tentang Kearsipan.
[15] Pasal 29 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
[16] Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.
[17] Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

perilakunya terlebih dahulu dan mengaturnya dari luar sistem melalui berbagai alat, cara dan metode. [18] Istilah *cybernetics* sendiri diterapkan dalam banyak teknologi, sehingga kemudian melahirkan banyak simbiosis antara manusia dengan teknologi. Konsep *cybernetics* ini pula yang kemudian melahirkan sebuah ruang atau dunia baru, yang tentunya memerlukan aturannya sendiri, ruang atau dunia inilah yang dinamakan dengan ruang siber (*cyberspace*).

Terminologi *cybernetics* sendiri dalam bahasa Indonesia sudah diserap menjadi sibernetika yang memiliki pengertian "ilmu pengetahuan tentang komunikasi dan pengawasan yang khususnya berkenaan dengan studi bandingan atas sistem pengawasan otomatis". Prefiks "siber" dari "sibernetika" ini kemudian dapat diambil dan diadaptasi untuk menterjemahkan *cyberspace*, *cybercrime* dan cyberlaw menjadi ruang siber, kejahatan siber dan hukum siber.[19] Pengunaan istilah siber juga lebih tepat karena merujuk pada konsep cybernetics sendiri yang merupakan penyatuan manusia dengan teknologi, yang kemudian melahirkan dunia tersendiri dalam *cyberspace* (ruang siber), tindakan kejahatan dalam dunia tersebut dalam *cybercrime* (kejahatan siber) dan membutuhkan norma hukum yang dapat tegas mengatur interaksi pada dunia tersebut dalam *cyberlaw* (hukum siber). Interaksi antara ketiganya dapat digambarkan dalam bagan berikut :



Gambar 1.1.
Bagan Hubungan Cyberspace, Cybercrime dan Cyberlaw (Diolah kembali dari Josua Sitompul, 2012 : 33)

[18] Lawrence Lessing, 2006, *Code*, Basic Books, New York, hal 6-7.
[19] Joshua Sitompul, 2012, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana*, Tatanusa, Jakarta, hal 14.

Sebagaimana dijelaskan di atas, internet telah membentuk ruang tersendiri untuk mewadahi aktivitas masyarakat, sehingga ruang baru tersebut juga membentuk perilaku-perilaku yang baru pula, termasuk perilaku kejahatan yang dinamakan dengan kejahatan siber. Berdasarkan Convention Cyber Crime 2001, kejahatan siber dibagi menjadi tiga kelompok : kejahatan terhadap sistem komputer, kejahatan terkait komputer dan kejahatan terkait konten komputer.[20] Komputer di sini bermakna pula jaringan antar komputer atau internet.

Sebagai sebuah bentuk kejahatan, hampir semua bentuk dari kejahatan siber merupakan kejahatan yang sebenarnya juga dikenal masyarakat di dunia fisik seperti pemalsuan, penipuan, pencurian, pencemaran nama baik, namun perbedaannya adalah menggunakan internet, merusak sistem di internet atau menyalahgunakan sistem di internet. Dengan kata lain, konsep dasar kejahatan siber merupakan efek samping internet sebagai bagian dari revolusi informasi.[21]

Kejahatan siber, memiliki karakteristik yang unik, tidak hanya dari ruang terjadinya dan pelaku, namun juga dari sisi korbannya. Secara umum terdapat beberapa bentuk viktimisasi kejahatan siber, yaitu[22] :

a. Akses tanpa ijin komputer seseorang
b. Penambahan data tanpa ijin komputer seseorang
c. Penghapusan atau perubahan data pada komputer seseorang tanpa ijin
d. Hilangnya data karena infeksi malware (virus)
e. Memiliki kartu kredit online orang lain tanpa ijin
f. Pelecehan online

Berdasarkan peraturan perundang-undangan di Indonesia terkait ruang siber pada UU ITE, telah diatur beberapa bentuk mengenai kejahatan siber di Indonesia. Pengaturan mengenai kejahatan siber atau dalam UU ITE disebut dalam Bab Perbuatan Yang Dilarang diatur dari Pasal 27 sampai dengan Pasal 37.

[20] Convention Cyber Crime Dewan Eropa Tahun 2001 Bagian Ke II.
[21] Ales Zavrsnik, 2008, *Cybercrime : Definitional Challenges and Criminological Particularities*, Masaryk University Journal of Law and Technology hal 2.
[22] Fawn T Ngo dan Raymond Paternoster, 2011, *Cybercrime Victimization: An Examination Of Individual And Situational Level Factors*, International Journal of Cyber Criminology Vol 5 Issue 1 hal 5.

2.4. Pelanggaran Privasi sebagai Kejahatan Siber

Dalam kasus cracking data ICloud artis Hollywood yang menyebarkan foto-foto telanjang mereka, pelakunya menggunakan teknik phising[23], dimana phising dilakukan dengan cara pelakunya menyebarkan e-mail yang dapat membobol sistem keamanan dari akun mereka. Namun phising sendiri hanyalah salah satu dari beberapa bentuk pelanggaran privasi di internet. Dalam kegiatan transaksi elektronik (e-commerce) terdapat beberapa bentuk pengumpulan informasi yang rawan atas pelanggaran privasi informasi pribadi yaitu[24] :

a. Teknik pemrosesan data dimana penyusunan data-data oleh pemerintah terkait dengan pengumpulan informasi penduduk
b. Pencarian data (*data mining*) melalui transaksi melalui internet maka informasi pribadi seseorang dapat dikumpulkan oleh pihak industri sehingga dapat diketahui hobi seseorang dan informasi barang-barang yang sering dibeli.
c. *Cookies* yaitu serangkaian teks yang dikirimkan oleh server ke penjelajah web untuk mengetahui situs-situs mana yang telah dikunjungi oleh seseorang sehingga dapat diketahui secara spesifik informasi seseorang tersebut.
d. *Web bug* adalah suatu alat perekam yang tersembunyi yang dapat merekam pesan-pesan email.
e. *Carnivore* adalah suatu alat yang dikembangkan oleh FBI untuk dapat memonitor email yang dikirim melalui atau menuju perusahaan penyedia jasa internet.

Dalam konteks penelitian ini mengenai pengiriman e-mail spam dan pelanggaran privasi, e-mail spam sendiri memang banyak menggunakan bentuk phising dimana terdapat informasi elektronik yang diterima namun mengandung gangguan terhadap sistem eletronik yang kita gunakan, sehingga dapat merusak atau mencuri data dan informasi elektronik yang kita miliki. E-mail spam memiliki perbedaan yang sangat tipis dengan *junk* e-mail dimana jumlahnya lebih besar, gangguannya lebih terasa dan lebih sulit dihindari karena bentuknya yang seperti e-mail biasa.[25] Karena beberapa aspek itulah e-mail spam cenderung melanggar batas-batas privasi individu, khususnya privasi di internet.

---

[23] Deliusno, 2016, *Begini Cara Peretas Curi Foto Bugil Jennifer Lawrence*, www.kompas.com (diakses 25 Maret 2016).
[24] Shinta Dewi, 2009, *Cyberlaw Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, Widya Padjajaran, Bandung, hal 35-36.
[25] Rob McCusker, 2005, *Spam : Nuisance or Menace, Prevention or Cure?*, Trends & Issues In Crime and Criminal Justice No. 294, Canberra, hal 2.

Beberapa negara sudah mengatur spam sebagai sebuah tindak pidana, dimana rata-rata spam digambarkan secara umum, tidak hanya pada konteks e-mail namun juga pada pengiriman informasi elektronik lainnya. Singapura mengatur spam sebagai kejahatan dalam Spam Control Act 2007 dimana dinyatakan bahwa spam adalah : "*Unsolicited commercial communications sent in bulk by electronic mail or by text or multi-media messaging to mobile telephone numbers, and to provide for matters connected therewith*"[26]

Sementara dalam EU Privacy Directive pengaturan mengenai spam dibagi ke dalam beberapa peraturan yaitu *The Distance Selling Directive*, *the E-Commerce Directive* dan *the E-Privacy Directive* [27]:

a. Dalam Distance Selling Directive, hak-hak konsumen dilindungi dalam hal privasi dari konsumen dengan mengatur cara-cara berkomunikasi antara produsen dengan konsumen, dimana salah satunya adalah komunikasi via e-mail yang dapat digunakan apabila tidak ada penolakan tegas dari konsumen.
b. Dalam E-Commerce Directive diatur tentang komunikasi terkait transaksi yang tidak diminta melalui e-mail, dimana setiap negara anggota dalam Directive ini diminta mengatur tentang identitas yang jelas dari pengirim e-mail (produsen)
c. Dalam E-Privacy Directive mengharmonisasikan aturan-aturan terkait, menyaring dan mengatur pula substansi dalam E-Commerce Directive dalam hubungannya dengan spam. E-Privacy Directive melarang pengiriman pesan komersial melalui fax, e-mail atau sistem telepon otomatis tanpa sepengetahuan penerima pesan sebelumnya.
d. E-Privacy Directives mengatur pula dua bentuk tindakan terkait pengiriman spam. Pertama, pelarangan pengiriman e-mail untuk promosi langsung dengan tujuan mengidentifikasi pengirim berdasarkan kepentingan yang terselubung. Kedua, e-mail untuk promosi atau pemasaran langsung tidak boleh dikirimkan tanpa alamat yang valid dimana penerimanya dapat meminta untuk menghentikan komunikasi tersebut.
e. E-Privacy Directives juga mengatur bahwa e-mail promosi atau pemasaran yang dikirimkan dapat menggunakan keterangan "advertisement" (iklan) yang tertera atau tercantum di dalam header e-mail tersebut, sehingga penerima dapat mengidentifikasi penting tidaknya e-mail tersebut.

[26] The Statutes of The Republic of Singapore Spam Control Act Act 21 of 2007.
[27] 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).

Dari uraian beberapa peraturan perundang-undangan di atas jelas bahwa di beberapa negara e-mail spam telah diatur sebagai sebuah kejahatan, khususnya kejahatan siber. Untuk dapat mengklasifikan pengiriman e-mail spam sebagai sebuah kejahatan tentu harus memenuhi unsur-unsur kejahatan terlebih dahulu. Dalam kaitan dengan kejahatan siber, secara unsur sama dengan kejahatan konvensional namun terdapat beberapa perbedaan dalam sarana atau alat yang digunakan motif dan karakteristik pelaku, serta karakter korban kejahatan siber.

Dalam aktivitas yang berhubungan dengan teknologi informasi kita bisa melihat pada bentuk transaksi elektronik, dimana menurut UU ITE transaksi elektronik adalah adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.[28] Dilihat dari pengertian di atas maka sebetulnya transaksi elektronik tidak hanya terbatas pada kegiatan jual-beli saja namun pada seluruh perbuatan yang memberikan akibat hukum.

Beberapa sistem elektronik atau website menyediakan kebijakan terkait privasi dari konsumennya sebagai contoh Facebook yang dalam menu *Privacy Policy*-nya mengatur tidak akan membagikan data atau informasi pengguna kecuali atas persetujuan pengguna, memberikan permberitahuan, bahwa hal tersebut termasuk dalam kebijakan terbaru dan menyamarkan identitas. Di sini berarti akibat hukum yang mungkin terjadi pada pengguna layanan Facebook dijamin oleh Facebook sebagai penyelenggara sistem elektronik terkait segala bentuk transaksi yang dilakukan oleh penggunanya, misalnya menggunakan aplikasi, game atau beberapa fitur yang memungkinkan data pribadi konsumennya akan diambil dan digunakan oleh Facebook. Hal ini berbeda dengan pengiriman e-mail spam, dimana salah satu ciri e-mail spam adalah "*unsolicited*" atau tidak diinginkan, dimana sebenarnya e-mail spam tersebut tidak diinginkan oleh penerima namun tetap dikirimkan.

Dalam kaitan kejahatan siber yang menggunakan sarana teknologi informasi dimana karakteristiknya sangat berbeda dengan kejahatan, maka perlu ditinjau lebih jauh apakah pelanggaran privasi melalui pengiriman e-mail spam dapat dikategorikan sebagai kejahatan, untuk menentukan apakah sebuah perbuatan merupakan kejahatan atau bukan maka dapat dilakukan melalui kriminalisasi. Dalam melakukan kriminalisasi tersebut perlu diperhatikan 4 hal berikut[29] :

a. Penggunaan hukum pidana perlu memperhatikan tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil dan makmur yang merata baik secara material

[28] Pasal 1 Angka 2 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[29] Sudarto, 1981, *Hukum dan Hukum Pidana*, Alumni, Bandung, hal 44-48.

maupun spiritual berdasarkan Pancasila. Penggunaan hukum pidana ditujukan untuk menanggulangi kejahatan dan mengadakan peng-ugeran terhadap tindakan penanggulangan itu sendiri, demi kesejahteraan dan pengayoman masyarakat.

b. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana seyogyanya merupakan perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian (material dan/atau spiritual) pada warga masyarakat.
c. Penggunaan hukum pidana perlu memperhitungkan prinsip "biaya dan hasil" (*cost and benefit principle*).
d. Penggunaan hukum pidana perlu pula memperhatikan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum pidana, jangan sampai ada kelebihan beban tugas.

Dalam mengkriminalisasikan pengiriman e-mail spam sebagai salah satu kejahatan siber, maka tentunya keempat hal tersebut harus diperhatikan, apakah sudah terpenuhi sehingga dapat menjadi dasar bagi pemerintah untuk melegalkan pengiriman e-mail spam sebagai salah satu bentuk kejahatan siber.

Apabila meninjau bentuk-bentuk tindak pidana yang sudah diatur dalam UU ITE, ada salah satu pasal yang berhubungan dengan gangguan seperti pengiriman e-mail spam, yaitu Pasal 33 UU ITE yang berbunyi "*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*." Dalam konteks pengiriman e-mail spam berbentuk phising, memang terdapat akibat berupa terganggunya sistem elektronik. Dalam hal delik materiil, Pasal 33 UU ITE ini pun maka akibat harus terjadi dari adanya perbuatan pidana tersebut.[30] Namun mengingat e-mail spam tidak hanya berakibat pada terganggunya sistem elektronik, namun juga adanya pelanggaran privasi dalam bentuk penyalahgunaan data maka tentu penentuan e-mail spam dalam UU ITE ini perlu dikaji lebih jauh.

Dalam Convention On Cybercrime 2001 sebagai instrumen hukum internasional yang mengatur kejahatan siber dalam empat modus yaitu *offences against the confidentiality, integrity and availability of computer data and system, computer related offences, content related offences* dan *offences related to infringement of copyright and related right*. Dari seluruh modus kejahatan siber tersebut pada dasarnya diawali dengan akses ilegal atau akses tidak sah dari pelaku kejahatan siber. Sehingga dapat dikatakan hampir seluruh bentuk

[30] Christian Adhi Nugroho S, Samsudi, Dwi Endah Nurhayati, 2013, *Op Cit*, hal 2.

kejahatan siber pasti diawali akses ilegal. Akses ilegal ini yang kemudian dapat berujung pada perusakan, pencurian, perubahan data atau sistem elektronik dalam kaitannya dengan pengiriman e-mail spam.

Akses ilegal sendiri dalam UU ITE diatur di dalam Pasal 30, yaitu modus hacking dan cracking. Dari segi kerugian sebetulnya cracking lebih berbahaya dibandingkan cracking karena cracking bertujuan mengambil atau merusak data sementara hacking lebih bertujuan menguji sebuah sistem sebagai bentuk unjuk kemampuan di dalam komunitas hacker. Namun dalam UU ITE diatur sebagai salah satu tindak pidana mengingat kemungkinan banyaknya modus kejahatan siber yang berawal dari akses ilegal.

BAB 3
TUJUAN DAN MANFAAT PENELITIAN

3.1. Tujuan Penelitian

Adapun berdasarkan rumusan latar belakang dan pertanyaan penelitian di atas, maka tujuan dari penelitian ini adalah sebagai berikut :

1. Mengetahui, memahami dan menganalisis e-mail spam sebagai salah satu kejahatan siber.
2. Mengetahui, memahami dan menganalisis pengaturan Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengenai pelanggaran privasi oleh e-mail spam.
3. Mengetahui, memahami dan menganalisis pengaturan yang ideal mengenai e-mail spam dalam kaitannya dengan perlindungan privasi pada hukum pidana siber Indonesia.

3.2. Manfaat Penelitian

1. Teoritis :

   Memberikan sumbangan pengetahuan kepada ilmu hukum e-mail spam sebagai salah satu jenis kejahatan siber.
2. Praktis :

   Menemukan gambaran yang jelas mengenai pengaturan yang ideal dan tepat dalam rangka melindungi privasi pengguna internet di Indonesia, khususnya terkait aktivitas e-mail spam yang menganggu privasi dalam UU ITE.

BAB 4
METODE PENELITIAN

4.1. Pendekatan 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 siber. Penelitian ini juga menggunakan pendekatan *Statute Approach* (Pendekatan Perundang-Undangan) untuk melihat pengaturan terkait e-mail spam sebagai bagian dari kejahatan siber serta *Comparative Approach* (Pendekatan Perbandingan) untuk melihat pengaturan e-mail spam di beberapa negara yang memiliki regulasi terkait.

4.2. Jenis dan Sumber Data

1. Data Primer

Data primer merupakan data yang didapatkan peraturan perundang-undangan terkait ruang siber (*cyberspace*) asas-asas dan pengaturan mengenai privasi di internet dan pengaturan mengenai e-mail spam apakah terdapat pengaturan mengenai e-mail spam.

2. Data Sekunder

Data sekunder merupakan buku literatur terkait dan jurnal-jurnal hukum yang membahas mengenai kejahatan siber 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.

4.3. Teknik Pengumpulan Data

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.

4.4. Teknik Analisa Data

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.

BAB 5
HASIL DAN PEMBAHASAN

5.1. E-mail Spam Didefinisikan sebagai Kejahatan Siber

Kejahatan siber merupakan fenomena global dan baru pada ranah hukum, khususnya hukum pidana, hal ini dikarenakan seiring dengan perkembangan teknologi informasi kejahatan pun berkembang bahkan melahirkan modus-modus baru pada kejahatan siber.

Pada awal perkembangannya, terminologi yang digunakan adalah kejahatan komputer peraturan perundang-undangan yang mengaturnya. 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 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.[31]

Penggunaan istilah "komputer" dalam mendefinisikan kejahatan terkait teknoogi informasi kemudian berubah dan berkembang menjadi kejahatan siber (*cyber crime*), khususnya sejak berlakunya Convention On Cyber Crime 2001, penggunaan terminologi "cyber crime" juga lebih tepat karena pada perkembangannya terdapat bentuk kejahatan yang tidak hanya berhubungan dengan komputer namun juga berhubungan dengan sistem atau jaringan komputer dan internet, bahkan banyak pula yang modus kejahatan yang menyerang data dan sistem komputer sebagai korban kejahatan siber.

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 Cyber Crime 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[32] :

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

[31] Andi Hamzah dan Boedi D. Marsita, 1987, *Aspek-Aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, hal 24.

[32] Hendry Chohwanadi, 2012, *Urgensi Kriminalisasi Terhadap Ketentuan Pidana Tentang "Spamming" Dalam Hukum Pidana Di Indonesia*, Artikel Ilmiah Fakultas Hukum Universitas Brawijaya, Malang, hal 2-3.

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 & 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.

Dari 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 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.[33]

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 spamming 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*.

[33] Shinta Dewi, 2009, *Perlindungan Privasi atas Infromasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, Widya Padjajaran, Bandung, hal 19.

Dalam Convention On Cyber Crime Tahun 2001 spam merujuk kepada *data interference* dan *system interference* dimana bersifat standar minimum dari rumusan perbuatan yang diatur di dalama Convention tersebut, sehingga setiap negara anggota dapat mengadopsi rumusan perbuatan tersebut untuk diatur sesuai dengan hukum domestik yang berlaku di negara mereka.[34]

Dalam rangka menetapkan sebuah perbuatan merupakan kejahatan siber, terdapat beberapa hal yang harus diperhatikan terkait kriminalisasi kejahatan siber, yaitu[35] :

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

Dalam rangka mengkriminalisasikan pengiriman e-mail spam sebagai kejahatan siber dan menyesuaikan apa yang diatur di dalam Convention Cyber Crime 2001 maka penulis akan merujuk pada tindak pidana *data interference* dan *system inteference* yang diatur di dalam hukum nasional, yaitu UU ITE.

5.2. 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 merugi atas pelanggaran privasi yang terjadi.

[34] Pasal 4 dan Pasal 5 Convention On Cybercrime 2001.
[35] Widodo, 2013, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta, hal 60-61

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.

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 siber 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.[36]

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.

[36] Adami Chazawi dan Ardi Ferdian, 2011, *Tindak Pidana Informasi & Transaksi Elektronik*, Bayumedia Publishing, Malang, hal 164-165.

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.[37]

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 pada pada 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 tersebut, dalam hal ini 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 spamming 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

[37]Budi Suhariyanto, 2012, *Tindak Pidana Teknologi Informasi (Cyber Crime) : Urgensi Pengaturan dan Celah Hukumnya*, Raja Grafindo Persada, Jakarta, hal 140.

konkret akan masuk ke dalam pengertian "melakukan kegiatan apapun" pada Pasal ini, asalkan perbuatan tersebut ditujukan pada suatu sistem elektronik.[38]

Apabila rumusan Pasal 33 UU ITE dibandingkan dengan rumusan *System Interference* dalam Convention Cyber Crime 2001, dari segi rumusan tidak jauh berbeda, namun Convention Cyber Crime 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 Cyber Crime 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*.[39]

Dalam rangka 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.[40] Dalam konteks Pasal-Pasal tindak pidana di UU ITE hampir seluruh modus kejahatan siber 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 siber ini tidak diawali oleh akses ilegal terlebih dahulu[41], 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

---

[38] Adami Chazawi dan Ardi Ferdian, *Op Cit*, hal 174.
[39] Widodo, 2012, *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law) : Telaah Teoritik dan Bedah Kasus*, Aswaja Pressindo, Yogyakarta, hal 62.
[40] 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 hal 4.
[41] Widodo, 2012, *Op Cit*, hal 55.

"*unsolicited*" di sini sangat subjektif[42], 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 siber pengiriman e-mail spam, maka akibatnya harus terjadi dulu. Dalam hal ini karena sifatnya yang subyektif makan sebagaimana pencemaran nama baik atau pengancaman maka 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.[43]

Dari 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 spamming 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 siber.

---

[42] 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 hal 5.
[43] *Ibid*.

5.3. Pengaturan Ideal Terkait E-Mail Spam sebagai Kejahatan Siber untuk Perlindungan Privasi dalam Hukum Pidana Indonesia

Sebagaimana telah diuraikan di atas, kejahatan siber 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 siber.

Pada 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.

Terdapat beberapa alasan yang dapat menjadi dasar suatu perbuatan untuk dikriminalisasi, yaitu [44]:

a. Adanya korban
b. Kriminalisasi bukan semata-mata ditujukan untuk pembalasan
c. Harus berdasarkan asas *ratio principle*
d. Adanya kesepakatan sosial

penulis akan membahas alasan-alasan tersebut satu-persatu berdasarkan unsur-unsur dan modus dalam pengiriman e-mail spam.

a. Adanya korban

Dalam 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.[45]

Sementara berdasarkan hasil riset dari ID CERT sampai bulan Desember 2015 pengaduan mengenai spam tercatat pada jumlah 41,7 % atau terdapat 16.087 pengaduan.[46] 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.

---

[44] Teguh Prasetyo, 2010, *Kriminalisasi dalam Hukum Pidana*, Nusamedia, Bandung, hal 45.
[45] Reska K Nistanto, 2015, *Jumlah E-mail "Sampah" di Indonesia Meningkat*, www.kompas.com (diakses 21 Maret 2016).
[46] ID CERT, 2015, *Laporan Dwi Bulanan VI 2015*, www.cert.or.id (diakses 17 Maret 2016).

Dalam konteks 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

Pada awal perkembangannya tujuan hukum pidana adalah untuk pembalasan atas kerugian yang dialami oleh korban. Namun pada konteks sekarang, khususnya yang berkaitan dengan kejahatan siber, 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 siber yang yurisdiksinya memungkinkan lintas batas negara, maka dibutuhkan strategi kebijakan non-penal dalam rangka memerangi kejahatan siber secara non-penal antara lain kerjasama internasional dan rencana aksi nasional dalam memerangi kejahatan siber.[47] 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.

Dalam hal 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 siber tersendiri.

d. Adanya kesepakatan sosial

Kesepakatan sosial di sini berasal dari pemerintah, dimana kriminalisasi merupakan kewenangan pemerintah dalam rangka menetapkan sebuah perbuatan diatur sebagai

[47] Widodo, 2013, *Memerangi Cybercrime : Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi*, Aswaja Pressindo, Yogyakarta, 147-148.

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 siber.

Pada dasarnya untuk mengkriminalisasikan pengiriman e-mail spam sebagai sebuah kejahatan siber, dapat dilihat pula dari permasalahan yang ditimbulkan, khususnya bagi para pihak atau pengguna teknologi informasi yaitu :

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)

Tabel 1.1.

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

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.

Dalam konteks 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. Dari 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[48].

[48] Evangelos Moustakas, 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), hal 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.

BAB 6
KESIMPULAN DAN SARAN

6.1. Kesimpulan

- Pengiriman *spam* biasanya bertujuan pada dua hal sebagai media promos 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.
- Pada dasarnya dalam 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.
- Pengaturan atau kriminalisasi pengiriman e-mail spam tentu harus memperhatikan ketiga unsur utama di atas, selain juga memperhatikan unsur-unsur dalam kriminalisasi, maka salah satu solusi yang dapat digunakan adalah dengan mengakomodir unsur-unsur spam di dalam peraturan perundang-undangan terkait, yaitu UU ITE.

6.2. Saran

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

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

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

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

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

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

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

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

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

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

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.

JURNAL DAN MAKALAH

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

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

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

Evangelos Moustakas, 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).

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

Graham Greenleaf, 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.

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

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

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

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

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

Christian Adhi Nugroho S, 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.

Dan Boneh, 2004, *The Difficulities 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).

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

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

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

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

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

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).

BIODATA PENELITI

A. Identitas Diri

1	Nama Lengkap	Eka Nugraha Putra SH., MH.
2	Jenis Kelamin	Laki-Laki
3	Jabatan Fungsional	Asisten Ahli
4	NIP	858/FH
5	NIDN	0721108602
6	Tempat dan Tanggal Lahir	Malang, 21 Oktober 1986
7	E-mail	eka.nugraha@unmer.ac.id
8	Nomor Telepon /HP	082110668824
9	Alamat Kantor	Jl. Terusan Raya Dieng 62-64
10	Nomor Telepon /Fax	0341-580161
11	Lulusan yang telah dihasilkan	S1 = 0 orang, S2 = 0 orang, S3 = 0 orang
12. Matakuliah yang diampu		1. Hukum Telematika
		2. Kejahatan Korporasi
		3. Hukum Perlindungan Konsumen
		4. Hak Atas Kekayaan Intelektual
		5. Hukum Internasional
		6. Hukum ASEAN
		7. Cyber Crime (Kejahatan Mayantara)

B. Riwayat Pendidikan

	S1	S2
Nama Perguruan Tinggi	Universitas Brawijaya	Universitas Indonesia
Bidang Ilmu	Hukum Pidana	Hukum dan Sistem Peradilan Pidana
Tahun Masuk-Lulus	2005-2009	2010-2012
Judul	Pengaturan Penggunaan Frekuensi Radio Untuk Penyelenggaraan Penyiaran Televisi Ditinjau Dari Aspek Hak Asasi Manusia Atas Informasi	Media Massa Dan Perannya Dalam Kebijakan Penanggulangan Kejahatan
Nama Pembimbing	Prof. Masruchin Ruba'i SH., MS. dan Eny Harjati SH., MH.	Prof. Topo Santoso SH., MH., PhD.

C. Publikasi Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/Nomor/Tahun
1	Kejahatan Tanpa Korban dalam Kejahatan Cyberporn	Jurnal Cakrawala Hukum Fakultas Hukum Universitas Merdeka Malang	Volume 6 / Nomor 1 / 2015

D. Pemakalah Seminar Ilmiah (Oral Presentation) dalam 5 Tahun Terakhir

No	Nama Pertemuan Ilmiah / Seminar	Judul Artikel Ilmiah	Waktu dan Tempat
1	Konferensi dan Dialog Nasional Negara Hukum 2012	*Keadilan Restoratif, Jalan Keluar Untuk Overkriminalisasi*	Hotel Bidakara Jakarta, 9-10 Oktober 2012
2	Second International Conference On Human Rights and Peace and Conflict in Southeast Asia 2012	*The Role Of Media In Reporting Human Rights Violation In Indonesia*	Hotel Millenium Sirih Jakarta, 17-18 Oktober 2012
3	The 3rd International Conference in conjunction with The 2nd International Conference on Multidisciplinary Research 2013	*Urgency of Regulating Cyberbullying on Indonesian Law*	Universitas Syiah Kuala Banda Aceh 2-4 October 2013
4	1st International Symposium on Regional Sustainable Development 2014	*To Ensure Victim Rights Protection of Corporate Environmental Crime*	Universitas Merdeka Malang 19 Juni 2014
5	International Conference In Indonesia-Australia Relations from the Perspective of International Law, Human Rights and Regional Security 2014	*Victim Rights Protection of Corporate Environmental Crime by Criminal Fine Sanctions*	Fakultas Hukum Universitas Airlangga Surabaya 23-24 September 2014
6	International Seminar and Human Rights Update “Freedom and Constitutionalism”	*When Consumer Complaint : The Border Between Freedom of Expression and Defamation*	Hotel Santika Pandegiling Surabaya 7-8 Desember 2015

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan Hibah Unggulan Perguruan Tinggi.

Malang , 12 April 2016

(Eka Nugraha Putra SH., MH.)