LEGITIMASI PENYEBARAN INFORMASI YANG MEMILIKI MUATAN PENGHINAAN DAN/ATAU PENCEMARAN NAMA BAIK DALAM PASAL 310 KUHP DAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK[1]

Oleh: Bima Guntara
Fakultas Teknik Universitas Pamulang
Jl. Surya Kencana Satu Pamulang Tangerang Selatan
Email: bimaguntara007@gmail.com

Abstrak

Keberadaan dunia *cyber* memberikan pengaruh besar di berbagai bidang kehidupan. Pengaruh tersebut tidaklah selalu berdampak positif tetapi juga negatif. Dampak negatif terwujudkan dengan istilah *cybercrime.* Perkembangan *cyber law* mengalami kemajuan pesat sehingga banyak pengaturan pada penggunaan dunia *cyber*. Tujuan penelitian ini adalah mengetahui legitimasi pemidanaan penyebaran informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik yang tidak dianggap salah oleh peraturan-peraturan lain di Indonesia kecuali oleh Undang-Undang ITE, dan mengetahui ketentuan penyebaran informasi dalam Pasal 27 ayat (3) Undang-Undang ITE merupakan pengaturan yang tepat untuk mengendalikan informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik. Hasil penelitian ini adalah legitimasi pemidanaan penyebaran informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik yang tidak dianggap salah oleh peraturan-peraturan lain di Indonesia kecuali oleh Undang-Undang ITE. Pasal 27 ayat (3) Undang-Undang ITE merupakan suatu ketentuan yang mengatur penyebaran informasi yang mengandung muatan penghinaan dan/atau pencemaran nama baik. Ketentuan penyebaran informasi dalam Pasal 27 ayat (3) Undang-Undang ITE belum bisa dikatakan sebagai pengaturan yang tepat untuk mengendalikan informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik di dalam teknologi informasi. Yang menjadi permasalahan bukanlah mengenai rumusan yang tidak jelas dan multitafsir yang terkandung dalam pasalnya, melainkan batasan dari ketentuan tersebut yang bisa dikatakan terlalu luas. Dengan penggunaan konsep penyebaran di dalam Pasal 27 ayat (3), maka setiap orang dapat dikenakan ketentuan tersebut dan dipidana karenanya. Hal ini akan mengakibatkan hilangnya kebebasan berekspresi dan kemerdekaan menyatakan pendapat baik secara lisan maupun tulisan.

Kata Kunci: Legitimasi, penyebaran informasi, penghinaan.

Abstract

The existence of the cyber world has had a major impact on many areas of life. The influence is not always positive but also negative. Negative impacts are realized by the

[1]Naskah diterima tanggal 2 Mei 2017, direvisi tanggal 2 September 2017, dan disetujui untuk diterbitkan tanggal 18 Oktober 2017 pada Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan Vol. 4 Nomor 2 Desember 2017.

term cybercrime. The development of cyber law is progressing rapidly so that many settings on the use of the cyber world. The purpose of this study is to know the legitimacy of criminalizing information dissemination that has defamation and / or defamation contents that are not considered wrong by other regulations in Indonesia except by the ITE Act, and know the provision of information dissemination in Article 27 paragraph (3) -The ITE is an appropriate setting for controlling information that has defamatory and / or defamatory content. The results of this study are the legitimacy of criminalizing information dissemination that has defamation and / or defamation contents that are not considered wrong by other regulations in Indonesia except by the ITE Act. Article 27 paragraph (3) of the ITE Law is a provision that regulates the dissemination of information containing contents of defamation and / or defamation. The provision of dissemination of information in Article 27 paragraph (3) of the ITE Act can not yet be regarded as an appropriate arrangement to control information having insulting and / or defamatory content in information technology. The problem is not about the unclear and multitafsir formulation contained in the article, but the limitations of those provisions which can be said to be too broad. With the use of the concept of dissemination in Article 27 paragraph (3), then any person may be subject to such provision and shall be liable for it. This will result in the loss of freedom of expression and freedom of expression of opinion both orally and in writing.
Keywords: Legitimacy, information spreading, humilition.

A. Latar Belakang Masalah

Cybercrime sebagai suatu masalah bukanlah hal yang mudah untuk diselesaikan. Hal ini dikarenakan c*ybercrime* sebagai suatu jenis kejahatan merupakan suatu tindakan yang dilakukan didalam dunia yang tidak mengenal batas wilayah hukum dan kejahatan tersebut dapat terjadi tanpa perlu adanya suatu interaksi langsung antara pelaku dengan korbannya. Sehingga dapat dikatakan, bahwa ketika suatu kejahatan *cyber* terjadi, maka semua orang dari berbagai negara yang dapat masuk kedalam dunia *cyber* dapat terlibat didalamnya, entah itu sebagai pelaku (secara langsung atau tidak langsung), korban, ataupun hanya sebagai saksi.

Oleh sebab itulah, untuk mengatasi atau setidaknya mengurangi masalah *cybercrime* ini, banyak negara-negara didunia yang mencoba melakukannya dengan membuat suatu pengaturan terhadap kejahatan tersebut yang dikenal dengan nama *cyber law*.

Cyber law ini merupakan suatu aspek hukum yang dimana ruang lingkupnya meliputi setiap aspek yang berhubungan dengan subyek hukum yang menggunakan dan memanfaatkan dunia *cyber* yang dimana biasanya pengaturan tersebut dimulai sejak

saat subjek hukum tersebut "*online*" dan memasuki dunia *cyber*.[2]

Pada negara yang telah maju yang dimana dunia *cyber* sangat begitu berpengaruh dalam berbagai bidang kehidupan mereka, perkembangan dari *cyber law* ini mengalami kemajuan yang sangat pesat sehingga terjadi banyak pengaturan pada penggunaan dunia *cyber* dalam negara-negara seperti itu. Salah satu contoh negara yang dapat digunakan untuk menerangkan bagaimana *cyber law* amat berkembang sebagai suatu aspek hukum dapat terlihat pada negara Amerika Serikat, yang dimana dalam negara tersebut setiap bidang kehidupan yang berhubungan dengan dunia *cyber* memiliki perangkat-perangkat hukum untuk melindungi warga negaranya.[3]

Di Indonesia, masalah dari *cybercrime* juga bisa dikatakan mulai diperhatikan sebagai suatu masalah yang serius. Dengan masuknya Indonesia kedalam era globalisasi, khususnya dalam hal hubungannya dengan dunia *cyber*, berbagai bidang kehidupan masyarakat Indonesia mulai mendapatkan pengaruh dari dunia *cyber* tersebut. Oleh karenanya tidaklah mengherankan bila mulai bermunculan kasus-kasus kejahatan yang berhubungan pula dengan dunia *cyber* tersebut.

Pada masa-masa awal munculnya berbagai kasus yang berkaitan dengan *cybercrime* di Indonesia, masalah ini merupakan masalah yang sangat sulit ditangani oleh Indonesia. Sebagai suatu negara yang masih baru dalam memasuki dunia *cyber*[4], pengaturan terhadap tindakan-tindakan yang berhubungan dengan *cybercrime* tersebut sangatlah kurang sekali.

Salah satu hal didalam Undang-Undang ITE yang menurut penulis dapat berupa kekurangan sehingga perlu untuk dibahas adalah mengenai pengaturan penyebaran informasi yang mengandung muatan penghinaan dan atau pencemaran nama baik. Dapat dikatakan demikian karena ketika pengaturan seperti itu tidak memiliki kepastian yang jelas mengenai apa yang sebetulnya diatur, maka terdapat kemungkinan terjadinya penyalahgunaan ketentuan oleh pihak-pihak tertentu yang dapat menghilangkan kebebasan berpendapat sebagai bagian dari hak asasi manusia[5].

[2]Ahmad Kamal, *The Law Of Cyber-Space***,** dapat dilihat dalam situ http://www.un.int/kamal/ thelawofcyberspace/diakses tanggal 23 Januari 2017.

[3] Beberapa contoh pengaturannya dapat dilihat dari situs http:// www.natlawreview. com/article/us- legislative- cybersecurity-update diakses tanggal 15 Februari 2008.

[4] Perkembangan sejarah dunia *cyber* di Indonesia dapat dilihat pada situs http://opensource. telkomspeedy. com/wiki/index.php/Sejarah InternetIndonesia, diakses tanggal 23 Januari 2017.

[5] Pasal 19 dari *The Universal Declaration of Human Rights*, dapat dilihat di situs http://

Oleh karena itulah, untuk dapat memahami apakah pengendalian informasi dengan muatan penghinaan dalam Undang-Undang ITE memiliki kekurangan atau tidak, penulis menjadikan pengaturan penyebaran informasi yang mengandung muatan penghinaan dan/atau pencemaran nama baik dalam Undang-Undang ITE sebagai suatu permasalahan (*statement of the problem)*.

B. Rumusan Masalah

Adapun yang menjadi pertanyaan tersebut adalah sebagai berikut:

1. Bagaimana legitimasi pemidanaan terhadap penyebaran informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik yang tidak dianggap salah oleh peraturan-peraturan lain di Indonesia kecuali oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ?
2. Bagaimana ketentuan penyebaran informasi dalam Pasal 27 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan pengaturan yang tepat untuk mengendalikan informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik ?

C. Metode Penelitian

Penelitian dalam tesis ini penulis lakukan berdasarkan metode penelitian:

1. Jenis Penelitian

Jenis penelitian ini dilakukan secara deskriptif analitis, yaitu metode penelitian yang dilakukan dengan cara melukiskan dan menggambarkan fakta-fakta baik data sekunder bahan hukum primer berupa peraturan perundang-undangan

2. Metode Pendekatan

Metode pendekatan yang digunakan adalah yuridis normatif, yaitu suatu metode yang mana hukum dikonsepsikan sebagai norma, kaidah, azas atau dogma-dogma. Metode pendekatan dalam penelitian ini menggunakan tiga pendekatan, yaitu pendekatan konsep (*conceptual approach),* pendekatan perundang-undangan (*statue*

www.un.org/en/documents/ udhr/ index.shtml diakses tanggal 11 Maret 2010.

approach), dan pendekatan kasus *(case approach)*.[6]

3. Sumber Data

Penelitian ini dilakukan dengan mencari data-data berupa:[7]

a. Bahan hukum primer, yaitu bahan-bahan hukum yang berupa Putusan Pengadilan, Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan peraturan perundang- undangan lainnya yang memiliki hubungan dengan penelitian.

b. Bahan hukum sekunder, yaitu bahan-bahan yang memberikan penjelasan mengenai bahan hukum primer, yang dimana berupa buku-buku yang berhubungan dengan permasalahan.

c. Bahan hukum tertier, yaitu bahan-bahan yang dapat memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder, yang dimana berupa kamus, ensiklopedia, dan internet.

4. Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui penelaahan data yang diperoleh dari perundang-undangan, putusan pengadilan, buku-buku teks, hasil penelitian, majalah, artikel, dan mengunjungi situs internet yang berhubungan dengan masalah penghinaan dan pencemaran nama baik.

D. Pembahasan

1. Tinjauan Umum Terhadap *Cybercrime*, *Cyber Law*, Legitimasi Penyebaran Informasi, dan Penghinaan

a. Pengertian *Cybercrime*

Ketika menjelajah dunia *cyber*, salah satu hal yang perlu diwaspadai adalah adanya kehadiran *cybercrime* dalam dunia *cyber* tersebut. Istilah *cybercrime* tersebut bisa dikatakan bukan istilah yang asing ketika kita sering menjelajah internet, namun, apakah yang sebetulnya dimaksud dengan *cybercrime* itu?

[6] Louis Cohen, Lawrence Manion, and Keith Morrison, *Research methods in education, (*London: Routledge Falmer ,2000), hal. 181.

[7] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, (Jakarta: Rajagrafindo Persada, 2003), hal. 13.

Istilah *cybercrime* (yang kadangkala diidentikan dengan istilah *computer crime*[8]*)* hingga tulisan ini ditulis belum memiki pengertian yang benar-benar pasti sehingga pengertian yang dimilikinya dapat bervariasi. Beberapa contoh pengertian tersebut dapat dijabarkan sebagai berikut:

1. Sarah Gordon dan Richard Ford dalam artikelnya yang berjudul *On The Definition and Classification of Cybercrime* memberikan definisi *cybercrime* sebagai "*any crime that is facilitated or committed using a computer, network, or hardware device*".[9]

2. Dalam *Convention on Cybercrime (EST no. 185)* yang dilakukan oleh Council of Europe, *cybercrime* dapat digunakan sebagai istilah untuk menjelaskan segala perbuatan melawan hukum yang berkaitan dengan komputer, seperti pencurian data, perusakan sistem komputer ataupun pelanggaran hak cipta.[10]

3. Bruce Middleton dalam bukunya yang berjudul *cybercrime Investigator Field Guide* menjelaskan *cybercrime* sebagai: "*a criminal offense that involves the use of a computer network."*[11]

4. Eoghan Casey dalam bukunya yang berjudul *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* menulis bahwa *cybercrime* merupakan istilah umum yang digunakan oleh organisasi-organisasi di dunia seperti U.S. Department of Justice (USDOJ) dan Council of Europe untuk memberikan pendefinisian secara luas terhadap kejahatan yang melibatkan komputer dan jaringan (*network*). Menurutnya, hal ini disebabkan karena apabila istilah *computer crime* yang digunakan, maka dapat timbul suatu kesulitan dalam pendefinisian ketika terdapat situasi dimana komputer atau jaringan (*network)* tidak terlibat secara langsung terhadap suatu perbuatan melawan hukum namun terdapat bukti digital (*digital evidence)* yang berhubungan dengan perbuatan melawan hukum

[8] C*ybercrime* kadangkala oleh beberapa orang diidentikan dengan *computer crime*, salah satu pendapat yang menyebabkan pengidentikan seperti itu adalah karena untuk melakukan *cybercrime* diperlukan komputer atau setidaknya peralatan yang mempunyai fungsi seperti computer.

[9] *Journal in Computer Virology Vol 2 No 1,* France: Springer-Verlag, 2006, hal. 14

[10] Didasarkan kepada tulisan dari: Krone, T., *High Tech Crime Brief,* Canberra: Australian Institute of Criminology, 2005, hlm. 1, dan *Convention On Cybercrime* yang didapatdarisitus:http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG.

[11] Bruce Middleton, *Cybercrime Investigator Field Guide: Second Edition, (*Florida: CRC Press, 2005), hal. 204.

tersebut. Misalkan saja ketika seorang pelaku perbuatan melawan hukum memberikan kesaksian bahwa dia sedang menjelajah internet pada saat peristiwa hukum terjadi, dalam hal ini, walaupun komputer yang digunakan untuk menjelajah internet tersebut tidak berhubungan langsung dengan perbuatan melawan hukum, namun komputer tersebut dapat merupakan alat bukti untuk membuktikan apakah kesaksian dari si pelaku benar atau tidak. Oleh karena itulah, untuk mempermudah pendefinisian karena adanya situasi seperti itu diperlukan penggunaan istilah yang dapat memiliki lingkup yang lebih luas daripada istilah *computer crime.*[12]

Dari beberapa pengertian tersebut, dapat dilihat bahwa walaupun dalam pendefinisiannya *cybercrime* memiliki persamaan, yaitu sama-sama terdapat hubungan dengan komputer, namun dalam ruang lingkupannya terdapat variasi dalam pendefinisiannya, ada yang secara luas memberikan ruang lingkupannya dan sebaliknya ada juga yang secara sempit mendefinisikannya. Selain itu pula, walaupun *cybercrime* dapat diidentikan dengan *computer crime*, bukan berarti bahwa *computer crime* juga selalu dapat diartikan sebagai *cybercrime*. Hal ini disebabkan karena *cybercrime* hanyalah bagian dari *computer crime* yang dimana dipengaruhi oleh eksistensi dari dunia *cyber.*

b. Jenis-Jenis *Cybercrime*

Setelah memahami secara umum mengenai apa yang dimaksud dengan *cybercrime*, hal lain yang menurut penulis perlu ditinjau adalah mengenai jenis- jenis dari *cybercrime*. Hal ini disebabkan karena menurut penulis dengan mengetahui jenis-jenis dari *cybercrime* dapat memberikan pemahaman mengenai apakah hal-hal yang diatur dalam Undang-Undang ITE sehingga dapat membantu dalam proses pembahasan masalah. Seperti yang telah dijelaskan pada bagian pengertian *cybercrime*, apa yang menjadi ruang lingkup dari *cybercrime* adalah hal-hal yang berhubungan dengan komputer, dengan demikian ketika *cybercrime* dikategorikan terdapat berbagai jenis *cybercrime*, antara lain:[13]

a. *Unautorized Access to Computer System and Service/Internet Intrusion.*
b. *Illegal Contents*

[12] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet: Third Edition*, (Maryland: Elsevier, 2011), hal. 37.

[13] Petrus Reinhard Golose, *Seputar Kejahatan Hacking: Teori dan Studi Kasus*, Jakarta: Dharmaputra, 2008, hlm. 30-42; dan Abdul Wahid dan Mohammad Labib, SH, *Kejahatan Mayantara (Cybercrime)*, Bandung: Refika Aditama, 2005, hal. 65-110.

c. *Data Forgery*
d. *Cyber Sabotage and Extortion*
e. *Offense Against Intellectual Property*
f. *Infringements of Privacy*
g. *Cracking / Hacking*
h. *Carding*
i. *Defacing*
j. *Phising/Indentity Theft*
k. *Spamming/Harassment Through E-Mails*
l. *Transmitting Malware*
m. *Cyber-child Pornography*[14]

c. Peraturan Perundang-undangan di Indonesia yang Dapat Dikaitkan dengan *Cybercrime* Selain Undang-Undang ITE

Sebelum adanya Undang-Undang ITE, tidak ada peraturan perundang-undangan di Indonesia yang mengatur secara khusus mengenai *cybercrime*. Oleh karenanya, dalam menangani kasus-kasus yang berkaitan dengan *cybercrime* pada masa sebelum adanya Undang-Undang ITE banyak digunakan peraturan perundang-undangan yang kiranya dapat dikaitkan dengan *cybercrime*, baik itu yang berasal dari KUHP maupun dari luar KUHP.[15] Undang-Undang ITE dapat dikatakan sebagai *cyber law* di Indonesia, namun sebetulnya apakah yang dimaksud dengan *cyber law* tersebut. Untuk membantu pemahaman, maka menurut penulis perlu dilakukan peninjauan secara umum terhadap *cyber law* tersebut serta hal-hal apa saja yang kira-kira dapat terkait dengannya.

Tinjauan Umum Mengenai *Cyber Law* dan Keterkaitannya dengan Undang-Undang ITE[16] Secara umum, *cyber law* dapat diartikan sebagai suatu hukum yang berkaitan dengan pemanfaatan teknologi. Dalam penerapannya kadangkala *cyber law* mengalami permasalahan dalam hal pembuktian dan penegakan hukum, hal ini

[14] Sultan Remy Syahdeini, *kejahatan dan Tindak Pidana Komputer,* (Jakarta: Pustaka Utama Grafiti, 2009), hal. 97.
[15] Petrus Reinhard Golose, *Seputar Kejahatan Hacking: Teori dan Studi Kasus,* (Jakarta: Dharmaputra, 2008), hal. 43.
[16] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*, (Jakarta: Rajagrafindo Persada, 2006), hal. 27-36 dan hal. 107-111.

dikarenakan ketidakjelasan batas wilayah hukum dalam dunia *cyber* sehingga suatu perbuatan melawan hukum dapat terjadi pada wilayah yang sangat berbeda dengan dimana pelaku itu berada.

Cyber law dapat diklasifikasikan sebagai ketentuan hukum yang berbeda dengan ketentuan hukum lain karena memiliki multi aspek yang dapat menguntungkan masyarakat dalam komunikasi yang mudah dengan menggunakan informasi elektronik. Namun disisi lain dapat merugikan karena hukum yang terkait belum mengatur secara jelas, dan belum cukup mampu memfungsikan dirinya sebagai sarana ketertiban.

2. Tinjauan Legitimasi Secara Umum Mengenai Penyebaran Informasi dalam Peraturan Perundang-Undangan di Indonesia[17]

Pengaturan mengenai penyebaran informasi dalam Undang-Undang ITE merupakan fokus utama dalam karya tulis ini. Oleh karena itu menurut penulis kiranya perlu dilakukan peninjauan secara umum mengenai apa yang dimaksud dengan penyebaran yang menjadi unsur dalam pengaturan penyebaran tersebut

Ketika meninjau mengenai penyebaran yang terdapat peraturan perundang-undangan di Indonesia, pemahaman mengenai penyebaran tersebut dapat didasarkan kepada *verspreiden delicten* yang digunakan oleh negara Belanda.

Hal ini disebabkan karena sistem hukum negara Indonesia dapat dikatakan merupakan peninggalan sistem hukum dari negara Belanda sehingga apa yang terkandung dalam delik-delik di Indonesia dapat dikaitkan dengan delik-delik yang ada di Belanda apabila tidak terdapat ketentuan yang dapat memberikan kejelasan mengenai pengertian.

Secara umum, dengan melihat dari kata *Verspreiden*, dapat ditafsirkan bahwa yang dimaksud dari kata tersebut adalah suatu tindakan penyebaran sehingga ketika dikaitkan dengan hukum maka bisa dikatakan hal-hal yang disebarkan oleh tindakan tersebutlah yang menciptakan suatu perbuatan melawan hukum.

Dengan kata lain, ketika seseorang menyebarkan sesuatu yang dilarang oleh hukum, maka dapat dikatakan dia telah melakukan suatu *verspreidings delict* atau suatu tindak pidana penyebarluasan.

[17] Lamintang, *Delik-Delik Khusus: Tindak Pidana- Tindak Pidana Melanggar Norma-Norma Kesusilaan dan Norma-Norma Kepatutan, (*Bandung: Mandar Maju, 1990), hal. 48-51.

3. Tinjauan Legitimasi Secara Umum Mengenai Penghinaan[18]

Dalam penelitian ini, hal yang diteliti adalah informasi yang mengandung muatan penghinaan, oleh karenanya perlu dilakukan peninjauan terhadap pengaturan secara umum terhadap penghinaan tersebut. Di Indonesia, karena ketentuan pidana secara umum diatur dalam KUHP, maka dalam hal penghinaan ini tinjauan terhadapnya dikaitkan dengan ketentuan yang diatur dalam KUHP tersebut.

Menurut Oemar Senoadji, pengertian penghinaan dapat diartikan sebagai perbuatan menyerang kehormatan atau nama baik "*aanranding of goede naam*" yang dimana dapat menimbulkan klasifikasi legislatif antara pencemaran tertulis (*smaadschriff*) yang merupakan penghinaan secara tertulis dengan menuduhkan sesuatu hal dan/atau penghinaan ringan yang merupakan penghinaan yang tidak mengandung pencemaran (tertulis) yang dilakukan terhadap seseorang.

Pengkategorian dalam pencemaran (tertulis) dan penghinaan ringan seringkali menunjukkan paralelitas seperti halnya pembagian antara "*defamation - insult*" ataupun "*diffimation" dan "injure*".

Ada tiga hal yang membedakan penghinaan biasa (*defamation-diffimation*) dengan penghinaan ringan, yang menimbulkan akibat hukum yang berbeda pula. Tiga hal tersebut ialah:

1. *Charge with and act or fact*, yaitu mengenai adanya tuduhan dari pelaku. Tuduhan demikian merupakan suatu persyaratan bagi penghinaan biasa yang tidak dijumpai pada "penghinaan ringan".

2. *Plea of justification*, yaitu hal yang dapat diajukan pada penghinaan biasa jika penghinaan yang terkait tidak dipersyaratkan pada penghinaan ringan.

3. *Proof of Truth*, yaitu mengenai istilah pembuktian akan kebenaran dari tuduhan yang dimana dapat dikaitkan dengan Pasal 311 KUHP yang memperbolehkan adanya pembuktian apabila hakim memandang perlu untuk memeriksa apakah perbuatan terdakwa dilakukan demi kepentingan umum atau karena terpaksa untuk membela diri. Unsur kepentingan kepentingan umum atau karena terpaksa untuk membela diri memiliki makna yang sama dengan Pasal 310 ayat (3) KUHP sehingga dapat dijadikan landasan untuk membenarkan suatu tindakan penghinaan. Oleh sebab

[18] Oemar Senoadji, *Perkembangan Delik Pers di Indonesia: Profesi Wartawan*, (Jakarta: Erlangga, 1991), hal. 37-42.

itu, ketika pelaku penghinaan menyadari bahwa dia melakukan penghinaan demi kepentingan umum (atau karena terpaksa membela diri), maka hakim memperkenankannya untuk membuktikan tentang kebenaran dari tuduhannya (*proof of truth*).

Penghinaan apabila dibagi berdasarkan ilmu hukum dapat dibedakan atas dua bagian, yaitu penghinaan materiil dan penghinaan formil. Yang dimaksud dengan penghinaan materiil adalah penghinaan yang isinya merupakan kenyataan atau fakta yang meliputi penyataan objektif (*zakelijk)* dalam kata-kata secara lisan ataupun tulisan. Hal ini menyebabkan isi dari penghinaan tersebut sebagai suatu faktor yang menentukan..

4. Kriminalisasi Penyebaran Informasi Dengan Muatan Penghinaan dan/atau Pencemaran Nama Baik dalam Undang-Undang ITE dan Ketentuan yang terkait Dengannya

Sebelum masuk kedalam pembahasan, ada baiknya menurut penulis dijabarkan terlebih dahulu mengenai ketentuan apa saja yang dapat dikaitkan dengan penyebaran informasi dan memiliki ruang lingkup yang sama dengan Undang-Undang ITE sehingga dapat diketahui ketentuan mana yang memiliki konsep penyebaran yang serupa. Melalui penjabaran tersebut diharapkan dapat membantu pengkategorisasian mengenai apakah legitimasi penyebaran yang terkandung dalam Undang-Undang ITE memiliki kesamaan dengan ketentuan lain yang dapat dikaitkan dengannya sehingga mempermudah penjelasan pada saat pembahasan.

Apabila ketentuan yang terkait didasarkan kepada apa yang telah ditinjau secara umum dalam bab 2, yaitu mengenai ketentuan yang terkait dengan *cybercrime* dan Undang-Undang ITE, maka pengkategorisasian lebih lanjut (dengan hanya melihat ada tidaknya unsur penyebaran dan unsur penghinaan) dari ketentuan-ketentuan tersebut menurut penulis hanya dapat dikategorikan menjadi 2, yaitu Undang-Undang ITE yang memuat ketentuan yang dibahas, dan KUHP yang merupakan ketentuan pidana yang memuat pemidanaan secara umum.

5. Pemahaman Legitimasi Penyebaran Informasi Dilihat Secara Tekstual[19]

Saat ini perkembangan teknologi informasi dapat dikatakan telah berkembang

[19] Jan Ifversen, *Text, Discourse, Concept: Approaches to Textual Analysis*, kontur nr. 7 – 2003, hlm. 61 – 69; *Textual Analysis - The Semiotic approach* dilihat dari situs http://www. godnose.co.uk/downloads/alevel/ textual%20analysis/semiotics.pdf>.

dengan pesat. Pesatnya perkembangan tersebut menyebabkan setiap orang dengan mudah memperoleh dan menyebarkan informasi yang dia miliki dalam wilayah yang sangat luas. Karena pesatnya perkembangan, adakalanya ketentuan hukum tertinggal dengan teknologi yang telah ada. Ketertinggalan ini dapat menyebabkan ketidakjelasan dalam batasan-batasan pengaturan yang dapat dikenakannya. Walaupun dalam penerapannya sebuah ketentuan hukum masih dapat digunakan, namun karena keterbatasannya pengaturan yang dikenakan dapat menjadi tidak tepat sasaran.

Apabila hal ini dijelaskan melalui contoh, maka salah satu contoh yang dapat digunakan adalah mengenai ketentuan mengenai pencurian. Ketika konsep kejahatan tersebut didasarkan pada KUHP, maka biasanya salah satu unsur yang diperhatikan adalah mengenai *mens rea* atau maksud dari perbuatan melawan hukum tersebut[20]. Namun dengan adanya internet sebagai akibat dari perkembangan teknologi informasi, *mens rea* kadangkala menjadi tidak berlaku. Hal ini disebabkan karena ketika seseorang mendapatkan suatu informasi dari internet, orang tersebut belumlah tentu mengetahui dengan jelas apakah informasi yang didapatkannya itu merupakan barang curian atau bukan, sehingga dengan demikian ketika dia menggunakan atau menyebarkan informasi tersebut tanpa memahami sepenuhnya isi dari informasi tersebut, maka tidak memungkinkan terdapat maksud untuk melakukan perbuatan melawan hukum olehnya.

Dengan melihat penjelasan melalui contoh tersebut penulis ingin mencoba menjelaskan bahwa hal yang serupa pun dapat terjadi kepada pengaturan penyebaran informasi dalam Undang-Undang ITE, khususnya dalam hal yang mengandung muatan penghinaan atau pencemaran nama baik. Karena adanya perkembangan teknologi informasi, Undang-Undang ITE dibuat untuk mengikuti perkembangan tersebut sehingga apabila terdapat perbuatan melawan hukum yang terkait dengan ruang lingkup dunia *cyber* diharapkan pengaturan melalui Undang-Undang ITE dapat tepat kepada sasarannya. Oleh karena itulah, untuk melihat seberapa tepat pengaturan melalui Undang-Undang ITE tersebut dilakukanlah tinjauan secara tekstual untuk melihat seperti apakah batasan dari konsep penyebaran informasi dalam Undang-Undang ITE jika dibandingkan dengan KUHP.

[20] *Actus reus Mens rea*, yang berarti dipidananya seseorang tidaklah cukup hanya apabila orang itu telah melakukan perbuatan yang bertentangan dengan hukum atau bersifat melawan hukum.

Seperti apa yang telah dijelaskan pada bab sebelumnya, konsep hukum mengenai penyebaran informasi KUHP dapat didasarkan kepada *verspreiden delicten* yang berasal dari sistem hukum negara Belanda, maka dapat dikatakan bahwa konsep hukum mengenai pengaturan penyebaran informasi yang digunakan dalam KUHP adalah apabila seseorang menyebarkan sesuatu yang dilarang oleh hukum dalam ruang akses yang luas sehingga setiap orang dapat memperoleh sesuatu yang disebarkan tersebut. Penggunaan konsep ini dalam KUHP biasanya tertuang dalam unsur yang berbunyi: diketahui umum/menyebarluaskan/disiarkan/dipertunjukkan/ditempelkan di muka umum. Karena penggunaan konsep yang sedemikian rupa, maka bila penyebaran informasi tersebut dilakukan dalam akses yang terbatas atau dalam lingkungan tertentu yang tidak memungkinkan banyak orang memasukinya, orang yang melakukan penyebaran tersebut tidak dapat dipidana.

6. Kasus Posisi

Untuk melakukan peninjauan melalui suatu kasus, menurut penulis cara peninjauan yang sesuai untuk digunakan adalah dengan melihat dari sebuah putusan yang telah mendapatkan kekuatan hukum tetap dan membahas kasus yang terkait dengan penyebaran informasi, khususnya mengenai informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik. Sehingga dengan demikian, dari putusan tersebut dapat dipahami bagaimana penerapan ketentuan yang mengatur penyebaran informasi yang memiliki muatan penghinaan dalam Undang-Undang ITE sehingga dapat membantu atau setidaknya memperkuat jawaban penulis untuk dapat menjawab pertanyaan yang diuraikan sebelumnya. Putusan dengan contoh kasus yang dipergunakan oleh penulis sebagai bahan pembahasan yaitu Nomor Putusan: 232/Pid.B/2010/PN.Kdl, yaitu sebagai Terdakwa Prabowo dan Saksi Korban Nur Dewi Alfiyana.

Pada awalnya antara Terdakwa dan Saksi Korban berkenalan sejak bulan Okotober 2007 dan berteman selama 2,5 (dua setengah) tahun kemudian karena kesibukan masing-masing antara Terdakwa dan Saksi Korban memutuskan untuk tidak berhubungan lagi sampai dengan tahun dimana kasus terjadi. Selanjutnya pada hari Jumat tanggal 01 Januari 2010 sekitar pukul 01.57 WIB karena sudah lama Saksi Korban tidak mendapat kabar dari Terdakwa, Saksi Korban mencoba mengirimkan pesan singkat yang isinya ucapan selamat tahun baru ke *handphone* milik Terdakwa

namun oleh Terdakwa pesan singkat tersebut tidak dibalas, kemudian keesok harinya Saksi K o r b a n mengirim pesan singkat lagi yang isinya menanyakan kapan Terdakwa akan menikah ke *handphone* milik Terdakwa namun oleh Terdakwa pesan singkat tersebut tidak dibalas.

Menimbang, bahwa unsur tersebut diatas seluruhnya merupakan unsur tindak pidana yang bersifat alternatif atau kumulatif, sehingga apabila salah satu unsur saja telah terbukti maka sudah dapat membuktikan seluruh unsur tindak pidana yang lainnya.

Menimbang, bahwa berdasarkan fakta yang terungkap di persidangan berdasarkan keterangan Saksi, pendapat Ahli, keterangan Terdakwa, keterangan Saksi Meringankan Terdakwa, keterangan Ahli Meringankan Terdakwa serta barang bukti yang diajukan dalam perkara ini terdapat persesuaian sehingga diperoleh fakta bahwa Terdakwa telah mengirimkan pesan singkat yang berbunyi "jangan ngaco dan ganggu orang bangsat lonte sekali lonte ya tetap lontelah, betapa rendah martabatmu ha. . kacian deh" dan "ya lagi2 diganggu bangsat lonte, dg sikapmu yg sprti itu pasti km akan selalu direndahkan org jadinya km tidak akan laku gitu nasehat sy te .. lonte" dari handphone milik Terdakwa kepada *handphone* milik Saksi Korban.

Menimbang, bahwa perbuatan Terdakwa mengirimkan pesan singkat dari *handphone* miliknya kepada *handphone* milik Saksi Korban yang berdasarkan fakta yang terungkap di persidangan, kemudian oleh Saksi Korban yang merupakan rekan kerja Saksi Korban, dan berdasarkan referensi yang dikeluarkan oleh Departemen Komunikasi dan Informasi Republik Indonesia (Depkominfo) dan pengertian Kamus Besar Bahasa Indonesia adalah dapat dikategorikan sebagai perbuatan mentransmisikan informasi elektronik dan/atau dokumen elektronik.

7. Legitimasi Pemidanaan Penyebaran Informasi Yang Memiliki Muatan Penghinaan dan/atau Pencemaran Nama Baik Yang Tidak Dianggap Salah Oleh Peraturan-Peraturan Lain di Indonesia Kecuali Oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Legitimasi pemidanaan penyebaran informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik yang tidak dianggap salah oleh peraturan-peraturan lain di Indonesia kecuali oleh Undang-Undang ITE. Pasal 27 ayat (3)

Undang-Undang ITE merupakan suatu ketentuan yang mengatur penyebaran informasi yang mengandung muatan penghinaan dan/atau pencemaran nama baik. Walaupun hanya sebuah pasal, unsur yang mengatur penyebaran dalam ketentuan tersebut dapat diidentikkan dengan semua pengaturan penyebaran di dalam Undang-Undang ITE. Hal ini dikarenakan bunyi dari unsur yang mengatur penyebaran tersebut memiliki persamaan, yaitu menyebarkan/ mendistribusikan/ mentransmisikan/ membuat dapat diaksesnya informasi.

Pasal 27 ayat (3) Undang-Undang ITE mengatur penyebaran informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik, melalui apa yang telah diuraikan dapat terlihat seperti apakah pengaturan penyebaran dalam Pasal tersebut. Oleh karena pengaturan yang sedemikian rupa, timbul suatu pertanyaan oleh penulis, apakah pengaturan penyebaran seperti itu diperlukan untuk mengatur informasi yang terdapat dalam bidang teknologi informasi khususnya dalam dunia cyber?

Ditinjau dari perjalanan sejarahnya, perlu tidaknya pengaturan informasi dalam Pasal tersebut dapat dilihat dari beberapa pendapat ahli hukum di Indonesia. Pendapat tersebut diantaranya:[21]

a. Menurut Edmon Makarim, Pasal 27 ayat (3) Undang-Undang ITE diperlukan agar sistem elektronik tidak menjadi ajang untuk saling mencemarkan nama baik karena dampaknya bersifat masif. Untuk menggunakan Pasal ini, penyidik dan jaksa penuntut umum haruslah dapat membuktikan dua unsur obyektif, yaitu dengan sengaja dan tanpa hak.

b. Menurut Muhammad Salahuddien Manggalany, Pasal 27 ayat (3) Undang-Undang ITE diperlukan karena bila dilakukan dengan teknologi informasi dampak kerusakan yang dihasilkan oleh tindakan yang diatur dalam Pasal tersebut bersifat meluas, jangka panjang dan dapat berulang sehingga kerugian yang dialami korban jauh lebih besar (efek amplifikasi) dibandingkan apabila dilakukan dengan saluran konvensional.

c. Menurut Sutan Remy Sjahdeini, Pasal 27 ayat (3) Undang-Undang ITE tidak diperlukan karena unsur "tanpa hak" dalam Pasal tersebut masih perlu dipertanyakan, yaitu mengenai ada tidaknya otoritas resmi yang memberikan hak bagi pihak tertentu untuk melakukan penyebaran informasi.

d. Menurut Adami Chazawi, Pasal 27 ayat (3) Undang-Undang ITE tidak diperlukan

[21]http://samardi.wordpress.com/2011/07/15/perdebatan-pasal-27-ayat-3-uu-ite/

karena pengaturan tindakan dalam Pasal tersebut masih bisa diatur dengan menggunakan pasal-pasal penghinaan di KUHP yang sesuai dengan kasusnya melalui penafsiran.

8. Ketentuan Penyebaran Informasi Dalam Pasal 27 ayat (3) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Merupakan Pengaturan Yang Tepat Untuk Mengendalikan Informasi Yang Memiliki Muatan Penghinaan dan/atau Pencemaran Nama Baik

Ketentuan penyebaran informasi dalam Pasal 27 ayat (3) Undang-Undang ITE belumlah bisa dikatakan sebagai suatu pengaturan yang tepat untuk mengendalikan informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik di dalam teknologi informasi. Yang menjadi permasalahan bukanlah mengenai rumusan yang tidak jelas dan multitafsir yang terkandung dalam pasalnya, melainkan batasan dari ketentuan tersebut yang bisa dikatakan terlalu luas..

Menganalisa kasus diatas maka dapat dibahas untuk memahami mengenai pengaturan penyebaran informasi. Oleh penulis apabila hal-hal tersebut dibahas dalam bentuk penjabaran, maka penjabaran tersebut dapat berupa sebagai berikut:

a. Penggunaan Pasal 27 ayat (3) Undang-Undang ITE

Putusan diatas menerapkan ketentuan penyebaran informasi dengan muatan penghinaan dalam Undang-Undang ITE.

b. Alat bukti yang digunakan

Alat bukti yang digunakan adalah informasi yang terdapat pada sebuah *handphone*. Menurut penulis alat bukti ini memiliki ruang lingkup akses yang terbatas yang dimana berarti tidak semua orang dapat dengan mudah mengetahui atau mendapatkan informasi darinya..

c. *Dolus eventualis* atau *opzet bij mogelijk heid bewustzejn*

Putusan diatas diterapkan *dolus eventualis* atau *opzet bij mogelijk heid bewustzejn* kepada Terdakwa. Maksud dari unsur semacam ini adalah bahwa pelaku melalui perbuatannya tidak bertujuan untuk melakukan suatu perbuatan melawan hukum walaupun terdapat kemungkinan bahwa dia tahu perbuatannya tersebut dapat

mengakibatkan suatu perbuatan melawan hukum.[22]

Yang menurut penulis menarik dibahas dalam hal ini adalah bahwa dalam putusan tersebut Terdakwa dianggap telah pasti tahu bahwa perbuatan yang dilakukannya berakibat melawan hukum. Padahal menurut Van Hattum kepastian dalam unsur kesengajaan tidak ada kepastian mutlak.[23] Sehingga ketika d*olus eventualis* digunakan perlu pula dipertimbangkan kemungkinan unsur lain dapat berbenturan dengannya, seperti *culpa* (kealpaan)[24].

d. Perbuatan dikategorikan sebagai mentranmisikan tetapi bukan mendistribusikan

e. Apakah yang dilakukan oleh Terdakwa dalam kasus yang ada merupakan suatu bentuk penyebaran dan apakah terhadapnya dapat dipidana

Melihat dari apa yang telah dijabarkan, dapat dilihat bahwa unsur distribusi dan tranmisi dapat dibedakan dalam penggunaannya, yang dimana apabila salah satu unsur tersebut terpenuhi maka dapat membuat valid ketentuan pengaturan tersebut. Sehingga dengan demikian perlu dilihat apakah perbedaan pengertian dari penyebaran dapat membuat suatu perbedaan dalam penafsiran.

E. Kesimpulan

Dari apa yang telah dibahas dalam bab sebelumnya, maka penulis mengambil simpulan sebagai berikut:

1. Legitimasi pemidanaan penyebaran informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik yang tidak dianggap salah oleh peraturan-peraturan lain di Indonesia kecuali oleh Undang-Undang ITE. Pasal 27 ayat (3) Undang-Undang ITE merupakan suatu ketentuan yang mengatur penyebaran informasi yang mengandung muatan penghinaan dan/atau pencemaran nama baik. Walaupun hanya sebuah pasal, unsur yang mengatur penyebaran dalam ketentuan tersebut dapat diidentikkan dengan semua pengaturan penyebaran di dalam Undang-Undang ITE. Hal ini dikarenakan bunyi dari unsur yang

[22] Wirjono Prodjodikoro, *Asas-Asas Hukum Pidana di Indonesia*. (Bandung: Eresco, 1989), hlm. 64-65; Sianturi, Op Cit., hal. 175.

[23] Wirjono Prodjodikoro, *Op Cit.*, hal. 63.

[24] Kesalahan pada umumnya, tetapi bisa juga diartikan sebagai suatu macam kesalahan pelaku tindak pidana yang terjadi karena kurang hati-hati sehingga menyebabkan akibat yang tidak disengaja. *Ibid*, hal 67.

mengatur penyebaran tersebut memiliki persamaan, yaitu menyebarkan/ mendistribusikan/ mentransmisikan/ membuat dapat diaksesnya informasi.

2. Ketentuan penyebaran informasi dalam Pasal 27 ayat (3) Undang- Undang ITE belumlah bisa dikatakan sebagai suatu pengaturan yang tepat untuk mengendalikan informasi yang memiliki muatan penghinaan dan/atau pencemaran nama baik di dalam teknologi informasi. Yang menjadi permasalahan bukanlah mengenai rumusan yang tidak jelas dan multitafsir yang terkandung dalam pasalnya, melainkan batasan dari ketentuan tersebut yang bisa dikatakan terlalu luas. Dengan penggunaan konsep penyebaran seperti yang diatur dalam Pasal 27 ayat (3), maka setiap orang dapat dikenakan ketentuan tersebut dan dipidana karenanya. Hal ini akan mengakibatkan hilangnya kebebasan berekspresi dan kemerdekaan menyatakan pendapat baik itu secara lisan maupun tulisan.

F. Saran

Dengan berdasarkan pada apa yang telah dikemukakan, penulis memberikan saran sebagai berikut:

1. Walaupun konsep penyebaran dalam Undang-Undang ITE dapat dijelaskan, namun batasan dalam ruang lingkup masih perlu dipertanyakan. Oleh karena itu penulis menyarankan untuk dilakukan penyempurnaan terhadap batasan-batasan mengenai pengaturan penyebaran dalam Undang-Undang ITE, misalnya seperti memasukan ke dalam Undang-Undang itu sendiri mengenai batasan yang diperlukan untuk didefinisikan sebagai perbuatan melawan hukum, menambahkan rumusan mengenai jenis penyebaran seperti apa yang dapat dikategorikan sebagai pelanggaran dan kejahatan, ataupun memberikan ketentuan mengenai apa yang dapat memberikan keringanan ataupun pemberatan.
2. Menurut penulis, pengaturan sanksi pidana secara khusus seperti halnya dalam Pasal 45 terhadap Pasal 27 ayat (3) Undang-Undang ITE sebetulnya tidak terlalu diperlukan apabila sudah terdapat ketentuan secara umum terhadap hal yang sama, sebab apabila terdapat pengaturan yang serupa terhadap suatu perbuatan dapat memungkinkan terjadinya konflik dalam pengaturan perbuatan

tersebut. Oleh karena itu penulis menghimbau agar ketentuan yang mengatur sanksi pidana tersebut dihilangkan atau diperbaiki sehingga tidak menimbulkan konflik dengan ketentuan lain yang mengatur hal yang serupa.

Daftar Pustaka

Buku

Arief, Barda Nawawi. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta:Rajagrafindo Persada, 2006.

Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet: Third Edition.* Maryland: Elsevier, 2011.

Cohen, Louis, Lawrence Manion, and Keith Morrison. *Research methods in education.* London: Routledge Falmer, 2000.

Golose, Petrus Reinhard. *Perkembangan Cybercrime dan Upaya Penanggulangannya di Indonesia Oleh Polri*. Bulentin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Jakarta, Agustus 2006.

Golose, Petrus Reinhard. *Seputar Kejahatan Hacking: Teori dan Studi Kasus.* Jakarta: Dharmaputra, 2008

Ifversen, Jan. *Text, Discourse, Concept: Approaches to Textual Analysis*.KONTUR nr. 7 – 2003.

Journal in Computer Virology Vol 2 No 1. France: Springer-Verlag, 2006.

Lamintang. *Delik-Delik Khusus: Tindak Pidana-Tindak Pidana Melanggar Norma-Norma Kesusilaan dan Norma-Norma Kepatutan.* Bandung: Mandar Maju, 1990.

Middleton, Bruce. *Cyber Crime Investigator Field Guide: Second Edition.* Florida: CRC Press, 2005.

Prodjodikoro, Wirjono. *Asas-Asas Hukum Pidana di Indonesia*. Bandung: Eresco, 1989.

Senoadji, Oemar. *Perkembangan Delik Pers di Indonesia: Profesi Wartawan*.Jakarta: Erlangga, 1991.

Soekanto, Soerjono dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajagrafindo Persada, 2003.

Syahdeini, Sultan Remy. *Kejahatan dan Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafiti, 2009.

Website

Krone, T., *High Tech Crime Brief*, Canberra: Australian Institute of Criminology, 2005, hlm. 1, dan *Convention On Cybercrime* yang didapat dari

situs:<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&D F=&CL=ENG

Beberapa contoh pengaturan tersebut dapat dilihat dari situs <http://www.natlawreview.com/article/us-legislative-cybersecurity-update. diakses tanggal 15 Februari 2008

Pasal 19 dari *The Universal Declaration of Human Rights*, dapat dilihat di situs < http:// www.un.org/en/documents/ udhr/ index.shtml diakses tanggal 11 Maret 2010

<http://samardi.wordpress.com/2011/07/15/perdebatan-pasal-27-ayat-3-uu-ite/

Ahmad Kamal, *The Law Of Cyber-Space***,** dapat dilihat dalam situs <http://www.un.int/kamal/thelawofcyberspace/>. diakses tanggal 23 Januari 2017

Perkembangan sejarah dunia *cyber* di Indonesia dapat dilihat pada situs <http://opensource.telkomspeedy.com/wiki/index.php/Sejarah_Internet_Indonesia, diakses tanggal 23 Januari 2017