PENEGAKAN HUKUM PIDANA TERHADAP AKSES SISTEM KOMPUTER SECARA ILEGAL (*HACKING)* DAN MENIMBULKAN KERUSAKAN (*CRACKING)* DALAM KEJAHATAN DUNIA MAYA (*CYBERCRIME)* MENURUT PERSPEKTIF UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

TESIS

Pembimbing :

1. **Dr. Ferdricka Nggeboe, S.H., M.H**
2. **Dr. Ruslan Abdul Ghani, S.H., M.H**

Disusun Oleh:
BENI SETIAWAN
NPM: B.16031074

PROGRAM MAGISTER ILMU HUKUM
UNIVERSITAS BATANGHARI
JAMBI
2019

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT atas limpahan rahmat dan karuniaNYA, Penulis dapat menyelesaikan penulisan tesis dengan judul ***"Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (Hacking) Dan Menimbulkan Kerusakan (Cracking) Dalam Kejahatan Dunia Maya (Cybercrime) Menurut Perspektif Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik"*** ini.

Tesis ini disusun adalah untuk memenuhi sebagian persyaratan untuk memperoleh Gelar Magister Ilmu Hukum pada Program Magister Ilmu Hukum Universitas Batanghari. Walaupun untuk menyusun tesis ini penulis telah mengerahkan kemampuan yang maksimal, akan tetapi disadari bahwa apa yang telah dicapai, tidaklah sesempurna apa yang diharapkan. Begitu pula sebagai insan biasa, penulis tidak mungkin bebas dari berbagai kekurangan dan kesalahan. Oleh karena itu, atas segala kekurangan dan kesalahan itu penulis menyampaikan permohonan maaf.

Terwujudnya tesis ini tidak terlepas dari bantuan dan bimbingan serta petunjuk dari berbagai pihak, kepada semuanya penulis haturkan terima kasih. Sehubungan dengan itu pula, penulis ingin menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya secara khusus kepada yang terhormat :

1. Bapak H. Fachruddin Razi, S.H., M.H, selaku Rektor Universitas Batanghari yang telah banyak memberikan motivasi dan kemudahan kepada penulis selama mengikuti pendidikan pada Universitas Batanghari;
2. Bapak Prof. Dr. Bari Azed, S.H., M.H, selaku Ketua Program Magister Ilmu Hukum Universitas Batanghari yang telah banyak memberikan bimbingan dan kemudahan kepada penulis selama mengikuti pendidikan pada Program Magister Ilmu Hukum Universitas Batanghari;
3. Ibu Dr. Suzanalisa, S.H., M.H, selaku Sekretaris Program Magister Ilmu Hukum Universitas Batanghari yang telah banyak memberikan bimbingan dan kemudahan kepada penulis selama mengikuti pendidikan pada Program Magister Ilmu Hukum Universitas Batanghari;

4. Ibu Dr. Fedricka Nggeboe, S.H., M.H dan Bapak Dr. Ruslan Abdul Ghani, S.H., M.H, selaku Pembimbing Pertama dan Pembimbing Keduayang telah banyak memberikan bimbingan dan arahan sehingga tesis ini dapat diselesaikan;
5. Bapak Ibu Dosen serta seluruh staf Tata Usaha Program Magister Ilmu Hukum Universitas Batanghari yang telah mendidik dan membimbing serta memberi kemudahan di bidang administrasi selama penulis mengikuti perkuliahan;
6. Kepada kedua orang tua, Bapak jaimun dan Siti Wasiah serta adiku satu-satunya Hartono yang telah banyak bersusah payah dan senantiasa berdoa sehingga penulis dapat menyelesaikan pendidikan pada Program Magister Ilmu Hukum Universitas Batanghari;
7. Rekan-rekan Program Magister Ilmu Hukum Universitas Batanghari angkatan Tahun Akademik 2016/2017 sebagai teman seperjuangan dalam menempuh pendidikan Strata Dua (S2) pada Program Magister Ilmu Hukum Universitas Batanghari;
8. Rekan-rekan kerja pada Institut Agama Islam (IAI) Nusantara Batang Hari, terutama kepada Rektor institut Agama Islam Agama Islam (IAI) Batang Hari yang telah banyak memotivasi memberi suport sehingga pendidikan Strata Dua (S2) penulis pada Program Magister Ilmu Hukum Universitas Batanghari dapat terselesaikan;

Atas segala bimbingan dan bantuan yang diberikan, semoga Allah SWT senantiasa melimpahkan rahmat NYA. Akhirnya penulis berharap semoga tesis ini dapat bermanfaat bagi semua pihak yang relevan hendaknya.

Jambi, Agustus 2019

Penulis

BENI SETIAWAN

NPM. B.16031074

ABSTRAK

Kemajuan teknologi yang sangat pesat, telah terbukti telah memberikan dampak positif bagi kehidupan manusia. Salah satu nya adalah terciptanya sebuah media baru untuk berinteraksi yang disebut internet *(cyberspace)*. Namun, perkembangan teknologi informasi saat ini menjadi pedang bermata dua, Karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Perbuatan melawan hukum dalam dunia maya tersebut lebih dikenal dengan *Cybercrime*. kejahatan dunia maya (*cybercrime*) itu adalah tindakan kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. Salah satu *cybercrime* yang berbahaya adalah akses sistem komputer secara ilegal (*hacking)* dan menimbulkan kerusakan (*cracking*). Pelaku kejahatan ini disebut *hacker* dan *cracker*. Penulis tertarik terhadap permasalahan ini dan mencoba menelaah berbagai sumber tentang *cybercrime* untuk meletakkan *hacking* dan *cracking* pada posisinya yang tepat. Selanjutnya mengkaji pasal-pasal dalam KUHP, KUHAP, beberapa Undang-undang, serta literatur serta kasus yang terkait langsung dengan *hacking* dan *cracking*, untuk diuraikan dan melihat bagaimana penegakan hukum terhadap kejahatan *hacking* dan *cracking* serta bagaimana aspek pembuktiannya. Penelitian yang dilakukan oleh penulis adalah penelitian deskriptif yang bersifat yuridis normatif, dengan menggunakan tiga macam pendekatan, yakni Pendekatan Perundang-undangan (*Statute Approach*), Pendekatan Konseptual (*Conceptual Approach*), serta Pendekatan Kasus (*Case Approach)*. Dari hasil kajian dapat disimpulkan bahwasanya meskipun didalam KUHP tidak menyebutkan secara *eksplisit* mengenai kejahatan *hacking* dan *cracking,* namun apabila dilihat dari Penafsiran *ekstensif* perbuatan tersebut dapat dipidana jika memenuhi unsur delik yang tercantum dalam pasal 167 dan 406 ayat (1) KUHP. Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik terdapat pengaturan Tindak Pidana *Hacking* dan *cracking* Pengaturan tindak pidana *hacking* dirumuskan pada Pasal 30 ayat (1), (2) serta (3) dan *cracking* Pasal 32 ayat (1) dan (3). Dalam aspek pembuktian terhadap kejahatan *hacking* dan *cracking* menurut Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik telah terjadi perluasan alat bukti sebagaimana yang sebelumnya telah diatur dalam KUHAP terdapat 5 (lima) alat bukti yakni Keterangan Saksi, Keterangan Ahli, Surat, Petunjuk dan Keterangan Terdakwa, maka ditambah satu alat bukti yaitu Informasi Elektronik dan Dokumen Elektronik. Inilah yang disebut dengan Alat Bukti Elektronik/alat bukti digital. Dalam kejahatan *hacking* dan *cracking, data log* yang tersimpan dalam server suatu jaringan *internet service protocol* (ISP) menjadi komponen penting dalam pembuktian sebagai upaya penegakan hukum terhadap *hacking* dan *cracking.*

Kata Kunci: *Tinjauan Hukum Pidana, Hacking, Cracking, Cybercrime*

ABSTRACT

The development of increasingly advanced technology, has been proven to have a positive impact on human life. One of them is the creation of new media for interaction called the internet (cyberspace). However, the development of information technology is now a double-edged sword, because in addition to contributing to improving the welfare, progress and human civilization, it is also an effective way to act against the law. Acts against the law in cyberspace are better known as Cybercrime. cybercrime is a criminal act carried out using computer technology as a primary crime tool. One dangerous cyber crime is illegal access to a computer system (hacking) and causing damage (hacking). Perpetrators of this crime are called hackers and crackers. The author is interested in this issue and tries to examine various sources of cyber crime to put hacking and cracking in the right position. Next review the articles in the Criminal Code, Criminal Procedure Code, several laws, as well as literature and cases that are directly related to hacking and hacking, to be elaborated and see how law enforcement against hacking and hacking of crime and how aspects of evidence. Research conducted by the author is a normative juridical descriptive study, using three types of approaches, namely the Statutory Approach, Conceptual Approach, and Case Approach. From the results of the study it can be concluded that although the Criminal Code does not explicitly mention the crime of hacking and cracking, but if viewed from a broad interpretation of these actions can be punished if it fulfills the violations listed in articles 167 and 406 paragraph (1) of the Criminal Code. Based on Law Number 11 Year 2008 Regarding Information and Electronic Transactions, there are provisions for Criminal Acts of Hacking and Cracking Hacking hacking rules are formulated in Article 30 paragraphs (1), (2) and (3) and cracks in Article 32 paragraphs (1) and (3). In the evidentiary aspect of the crime of hacking and cracking according to Law Number 11 of 2008 concerning Information and Electronic Transactions there has been an expansion of evidence as stipulated in the Criminal Procedure Code there are 5 (five) pieces of evidence namely Witness Statement, Expert Statement, Letter, Instruction and Defendant's Statement , then add one proof, namely Electronic Information and Electronic Documents. This is called Electronic Proof / digital proof. In a crime of hacking and hacking, log data stored on an internet service protocol (ISP) network server becomes an important component in verification as an effort to enforce law against hacking and hacking.

Keywords: *Criminal Law Review, Hacking, Cracking, Cybercrime*

DAFTAR ISI

HALAMAN JUDUL i

HALAMAN PERSETUJUAN ..... **i**

HALAMAN PENGESAHAN ..... **ii**

KATA PENGANTAR ..... **iii**

ABSTRAK ..... **v**

ABSTRACT ..... **vi**

DAFTAR ISI ..... **vii**

BAB I PENDAHULUAN 1
A. Latar Belakang Masalah 1
B. Rumusan Masalah 12
C. Tujuan dan Manfaat Penelitian 12
D. Kerangka Konseptual 14
E. Kerangka Teori 17
F. Metodologi Penelitian 27
G. Sistematika Penulisan 32

BAB II TINJAUAN UMUM TENTANG KEJAHATAN DUNIA MAYA (*CYBERCRIME*) **35**
A. Defenisi Kejahatan Dunia Maya *(Cybercrime)* 35
B. Jenis-Jenis Kejahatan *Cybercrime* 42
C. Unsur-unsur Tindak Pidana dalam *Cybercrime* 53
D. Pengaturan Hukum *Cybercrime* di Indonesia 59
E. Ruang Lingkup *Cybercrime* 77

BAB III AKSES SISTEM KOMPUTER SECARA ILEGAL (*HACKING*) DAN MENIMBULKAN KERUSAKAN (*CRACKING*) DALAM HUKUM PIDANA DI INDONESIA **80**
A. Defenisi *Hacking* dan *Cracking* 80
B. Tahapan-tahapan dalam Melakukan *Hacking* dan *Cracking* 86

C. Faktor – Faktor yang Mempengaruhi Terjadinya *Hacking* dan *Cracking* 92
D. Konstruksi *Hacking* dan *Cracking* Sebagai Kejahatan *Cybercrime* 99
E. Pengaturan Hukum Pidana Terhadap *Hacking* dan *Cracking* menurut KUHP 103
F. Aspek Yurisdiksi pada Tindak Pidana *Hacking* dan *Cracking* 108

BAB IV PENEGAKAN HUKUM PIDANA TERHADAP PELAKU AKSES SISTEM KOMPUTER SECARA ILEGAL (*HACKING)* DAN MENIMBULKAN KERUSAKAN (*CRACKING)* 121
A. Penegakan Hukum pidana Terhadap Pelaku Kejahatan *hacking* (*hacker*) dan *Cracking* (*cracker*) 121
B. Aspek Pembuktian Terhadap Tindak Pidana *Hacking* Dan *Cracking* 143

BAB IV PENUTUP
A. Kesimpulan 154
B. Saran 156
C. Penutup 157
DAFTAR PUSTAKA 159

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi memegang peran penting, baik di masa kini maupun di masa mendatang. Kemajuan teknologi informasilah yang menyebabkan ledakan kemajuan peradaban manusia, ledakan impian yang menjadi kenyataan. Bila mengkaji tentang kemajuan teknologi informasi, maka tidak dapat dipisahkan dari perkembangan teknologi komputer dan internet. Komputer dan Internet sebagai penemuan yang begitu mengagumkan merupakan awal dari pencapaian apa yang telah manusia rasakan saat ini. Sebab, komputer dan internet telah merubah budaya manusia dari budaya industri menjadi budaya yang berlandaskan informasi. Budaya di mana informasi menjadi kebutuhan penting, dapat diakses tak terbatas dan tanpa batas (*Borderless*).

Internet telah menciptakan dunia baru yang disebut dengan *cyber space* yaitu dunia komunikasi yang berbasis komputer yang menawarkan realitas yang baru yang berbentuk virtual (tidak langsung dan tidak nyata). Secara etimologis, *istilah cyber space* sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir. *Cambridge Advanced Learner's Dictionary* memberikan definisi *cyberspace* sebagai *"the Internet considered as an imaginary area without limits where you can meet people and discover information about any subject"* atau Internet dianggap sebagai wilayah imajiner

tanpa batas di mana Anda dapat bertemu orang-orang dan menemukan informasi tentang subjek apapun.[1] *The American Heritage Dictionary of English Language Fourth Edition* mendefinisikan *cyberspace* sebagai "*the electronic medium of computer networks, in which online communication takes place*" atau Media elektronik jaringan komputer, di mana komunikasi online berlangsung.[2]

Dengan adanya internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. munculnya dunia virtual ini telah mengubah kebiasaan banyak orang terutama dalam kehidupannya terbiasa menggunakan Internet. Mulai dari mengubah cara dan sarana transaksi bisnis atau transaksi perbankan yang dilakukan dengan menggunakan Internet yang berlangsung di dunia virtual disebut dengan transaksi elektronik *(electronic transaction atau e-commerce)*, pendidikan (*electronic education*), kesehatan (*tele-medicine*), telekarya, transportasi, industri parawisata, lingkungan, sampai dengan sektor hiburan. Teknologi informasi dengan sendirinya juga merubah perilaku masyarakat.

Namun dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri. Perkembangan komputer dan internet tidak dapat dipungkiri telah menjadi sarana atau ladang baru bagi dunia kejahatan. Sebab komputer dan internet sebagai ciptaan manusia memiliki karakteristik mudah

---

[1]Cambrige Dictinory, *Meaning of **cyberspace** in English*, https://dictionary.cambridge.org/dictionary/english/cyberspace?q=Cyber+space, diakses tanggal 28 April 2019

[2]The American Heritage Dictionary of the English Language, *Meaning of **cyberspace** in English* Fifth Edition, https://www.ahdictionary.com/word/search.html?q=cyberspace diakses tanggal 28 April 2019

dieksploitasi oleh siapa saja yang memiliki keahlian di bidang tersebut. Sehingga dapat dikatakan perkembangan teknologi informasi saat ini menjadi pedang bermata dua, Karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.[3] Perbuatan melawan hukum dalam dunia maya tersebut lebih dikenal dengan *Cybercrime.*

Secara singkat *Cybercrime* dapat diartikan dengan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan.[4] Namun ada juga yang berpendapat bahwa kejahatan dunia maya (*cybercrime*) itu adalah tindakan kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime* merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet. *Cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh bidang kehidupan modern saat ini.[5]

Jenis tindak pidana *Cybercrime* terbagi dalam dua jenis, yaitu kejahatan dengan motif intelektual. Biasanya jenis yang pertama ini tidak menimbulkan kerugian dan dilakukan untuk kepuasaan pribadi. Jenis kedua adalah kejahatan

---

[3] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi dan Pengaturan Celah Hukumnya*, Jakarta: Raja Grafindo Persada, 2012, halaman 2.

[4] Wikipedia, *Pengertian Kejahatan Dunia Maya*, https://id.wikipedia.org/wiki/Kejahatan_dunia_maya diakses tanggal 24 Mei 2019.

[5] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: PT Raja Grafindo Persada, 2007, halaman 1.

dengan motif politik, ekonomi atau kriminal yang berpontesi menimbulkan kerugian bahkan perang informasi. Yang termasuk jenis tindak pidana komputer tersebut diantaranya adalah *cybersquatting, identity theft,* kejahatan kartu kredit *(carding)*, *phising, hacking, cyberterrorism, DOS-DDOS attack, online gambling,* penyebaran *malware,* pencurian data dan informasi eletronik, memodifikasi data dan informasi elektronik, pengadaan program komputer secara tidak sah, pornografi anak (*child pornography), cyberstalking* dan penyebaran berita bohong (*Hoax*).[6]

Cybercrime mempunyai banyak bentuk atau rupa, tetapi dari kesemua bentuk yang ada, *hacking* merupakan bentuk yang banyak mendapat sorotan, karena selain kongres PBB X di Wina menetapkan *hacking* sebagai *first crime*, juga dilihat dari aspek teknis, *hacking* mempunyai kelebihan-kelebihan. Pertama, orang yang melakukan *hacking* sudah barang tentu dapat melakukan bentuk *cybercrime* yang lain karena dengan kemampuan masuk ke dalam sistem komputer dan kemudian mengacak-acak sistem tersebut. Termasuk dalam hal ini, misalnya *cyber terrorism, cyber pornography* dan sebagainya. Kedua, secara teknis pelaku *hacking* kualitas yang dihasilkan dari *hacking* lebih serius dibandingkan dengan bentuk *cybercrime* yang lain, misalnya pornografi.

Pada awal mulanya, sekitar tahun 1960 *Hacker* diartikan sebagai orang yang gemar mempelajari sistem komputer dan bereksperimen dengannya.[7] *Hacker-Hacker* ini adalah *Hacker* yang berasal dari *Massachushet Institute*

---

[6] Sutan Remy Syahdeini, *Kejahatan & Tindak Pidana Komputer*, Jakarta: Pustaka Utama Grafiti, 2009, halaman 8.

[7] Budi Raharjo, Keamanan Sistem Informasi Berbasis Internet, PT Insan Indonesia, Bandung, 1998-2005, halaman 5-6

Technology (MIT). Para *hacker* ini mempunyai etika dan motivasi bahwa menghack adalah untuk tujuan meningkatkan keamanan jaringan internet. Penggunaan istilah *hacker* terus berkembang seiring perkembangan internet dan terjadi pembiasaan terhadap makna *hacker* tersebut. *Hacker* yang masih memiliki etika dan motivasi sama dengan perintis mereka *(Hacker-hacker dari MIT/Old School*) disebut sebagai *hacker* topi putih *(White Hat Hacker)*.

Namun seiring lunturnya etika *hacker* itu sendiri, sekarang dampak yang ditimbulkan antara *hacker* dan *cracker* yang hampir sama. Hal ini dapat dilihat dari perilaku *hacker* yang meskipun tidak melakukan perusakan tapi melakukan data-data pemerintah dan perbankan. Secara umum tindakan lebih dapat ditolerir karena tidak merusak data atau sistem yang di *hack,* kemudian si *hacker* memberi tahu bahwa sistem tersebut rentan penyusupan. Dalam suatu kasus kadang-kadang penyusupan *hacker* ini tidak diketahui oleh *host* (pemilik situs), sehingga host tetap merasa sistem security nya aman. Tentu hal ini hanya dapat dilakukan oleh *hacker-hacker* topi putih (*white hat hacker*). Lagi-lagi karena menurunnya etika dalam segala aspek maka kemudian eksistensi *white hat hacker* patut dipertanyakan.

Hacker secara umum dapat diartikan seseorang yang mempunyai kemampuan lebih di bidang keamanan jaringan komputer dan memanfaatkan kemampuannya untuk mendapatkan akses secara ilegal kedalam sistem komputer orang lain. Jika tindakan yang dilakukan bersifat *destruktif*, merugikan pihak lain

istilah yang lebih tepat adalah *Cracker.*[8] Istilah *hacker* sendiri masih belum baku karena sebagian menganggap *hacker* mempunyai konotasi yang positif , dan sebagian mengkonotasikan negatif. Batas antara *hacker* dan *cracker* sangat tipis. Batasan ini ditentuka oleh etika, moral, dan integritas dari pelaku itu sendiri.[9]

Fenomena kejahatan *hacking* dan *cracking* memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. Tindak pidana *Hacking* dan *cracking* dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas perkembangan tindak pidana komputer ini.

Sebelum diundangkan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Modus kejahatan dalam dunia *cyber* memang agak sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan teknologi informasi dalam modus operandinya. Sifat ini membuat *cybercrime* berbeda dengan tindak pidana lainnya.[10] Maka apabila di Indonesia ada seseorang yang melakukan perilaku kejahatan di dalam internet sebagai sasaran utama kejahatannya atau menggunakan program internet maka diterapkan Kitab Undang Hukum Pidana sebagai Undang-undang pidana umum. Tentu saja hal tersebut

---

[8] Computer Network Research Group, *Mengejar Hacker itu Mudah, Bandung*, 20 Mei 2004

[9] Budi Raharjo, *Op. cit*., halaman 24.

[10] Mardjono Reksodiputro, *Kejahatan komputer (Suatu catatan sementara dalam rangka KUHP Nasional yang akan datang) , dalam Kemajuan Pembangunan Ekonomi dan Kejahatan*, Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum UI, 1997, halaman 10.

dapat dilakukan sepanjang KUHP ditemukan pasal – pasal yang pas dan tepat untuk menjatuhkan pidana.

Demi merespon atas berkembanganya hal tersebut maka Indonesia memasukkan materi tindak pidana *cyber* sebagai salah satu materi delik dalam Rancangan Kitab Undang-undang Hukum Pidana (R-KUHP) Nasional. Dalam draft R KUHP Nasional 2010 Tindak Pidana terhadap Informatika dan Telematika. Dalam R KUHP Nasional 2010 juga dilakukan redefinisi tentang Barang (Pasal 165)[11], Surat (Pasal 207)[12], Masuk (Pasal 186).[13]

Di Indonesia sendiri, ada dua undang-undang yang dapat mengatur tentang informasi dan transaksi elektronik yang berlaku di Indonesia. Yang pertama adalah Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi sedangkan yang kedua adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), kemudian undang-undang ini di revisi menjadi Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Undang-undang tersebut dikeluarkan karena telah banyak yang bermunculan kejahatan-kejahatan di dunia maya di Indonesia yang sangat merugikan perorangan maupun masyarakat luas. Ada beberapa Undang-undang lainnya yang terkait dengan tindak pidana *cyber* seperti Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Undang-undang

[11] Barang adalah benda berwujud termasuk air dan uang giral dan benda tidak berwujud termasuk aliran listrik , gas , data dan program komputer , jasa termasuk jasa telepon , jasa telekomunikasi atau jasa komputer.

[12] Surat adalah surat yang tertulis diaatas kertas, termasuk juga surat atau data yang tertulis atau tersimpan dalam disket, pita magnetik , atau media penyimpan komputer atau media penyimpan data elektronik lain.

[13] Masuk adalah termasuk mengakses komputer atau masuk kedalam sistem komputer

Nomor 19 Tahun 2002 tentang Hak Cipta yang mengatur perlindungan *software* komputer dan menetapkan sanksi pidana bagi yang melanggarnya.

Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik memilih mengacu model yang bersifat komprehensif artinya materi muatan yang diatur di dalamnya mencakup hal yang luas disesuaikan dengan kebutuhan saat ini. Dalam Undang-undang tersebut terdapat beberapa pasal pidana yang merupakan ketentuan pidana khusus disamping berlakunya KUHP sebagai Undang-undang tindak pidana umum. Sedangkan Undang-undang Nomor 36 Tahun 1999 tentang telekomunikasi merupakan pengganti dari Undang-undang sebelumnya yaitu Undang-undang Nomor 3 Tahun 1989 tentang Telekomunikasi. Undang-undang ini dilahirkan sebagai konsekuensi dari adanya perubahan mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi yang memerlukan penataan dan pengaturan kembali penyelenggaraan telekomunikasi nasional.

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang merupakan *lex generalis* dari Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik belum secara spesifik mengatur hal-hal yang berkaitan dengan telekomunikasi dengan Internet. Sama halnya dengan Kitab Undang Hukum Pidana yang sangat terbatas sekali untuk diterapkan terhadap tindak pidana *cyber,* khususnya dalam *hacking* dan *cracking*.

Pemerintah Indonesia telah berupaya dengan membuat berbagai macam regulasi dan peraturan untuk menghadapi akibat yang timbul dari kegiatan *hacking* dan *cracking*. Itu dibuktikan dari gigihnya aparat dengan mencoba menjerat *hacker* dan *cracker* dengan hukum pidana yang berlaku. Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ini diharapkan mampu menjawab berbagai persoalan yang timbul dari kasus yang menyangkut teknologi informasi, termasuk *hacking* dan *cracking*, meskipun Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik tidak secara eksplisit menyebut *hacking* dan *cracking* di dalamnya. Selain itu, lahirnya Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik diharapkan menjadi jawaban dari lemahnya KUHP, KUHAP dan UU terkait yang dipandang sudah tidak mampu lagi menjawab berbagai permasalahan yang timbul dari penerapan teknologi informasi di masyarakat.

Selain itu dalam penanganan Kejahatan *hacking* dan *cracking* Masalah Pembuktian memiliki karakteristik tersendiri. Dalam hal ini sifat alami dari teknologi komputer memungkinkan pelaku kejahatan untuk menyembunyikan jejaknya. Untuk menghindari jeratan hukum *hacker* dan *cracker* tidak bodoh, Agar *hacker* terlindungi pada saat melakukan serangan, teknik cloacking (penyamaran) dilakukan dengan cara melompat dari mesin yang sebelumnya telah di compromised (ditaklukan) melalui program telnet atau rsh. Pada mesin

perantara yang menggunakan Windows serangan dapat dilakukan dengan melompat dari program *Wingate / proxy server*. Selanjutnya *hacker* harus mengidentifikasi komponen jaringan yang lemah dan bisa ditaklukan. *Hacker* bisa menggunakan program di *Linux* seperti *ADMhack, mscan, nmap* dan banyak scanner kecil lainnya. Program seperti *'ps' & 'netstat'* di buat *trojan* untuk menyembunyikan proses *scanning*.

Setelah *hacker* berhasil mengidentifikasi komponen jaringan yang lemah dan bisa ditaklukan, maka *hacker* akan menjalankan program untuk menaklukkan program *daemon* yang lemah di *server*. Program *daemon* adalah program di *server* yang biasanya berjalan di belakang. Keberhasilan menaklukan program daemon ini akan memungkinkan seorang *Hacker* untuk memperoleh akses sebagai 'root' (administrator tertinggi di *server*). Untuk menghilangkan jejak, seorang *hacker* biasanya melakukan operasi pembersihan *'clean-up'* operation dengan cara membersihkan berbagai *log file*. Dan selanjutnya menambahkan program 'backdooring' dengan cara Mengganti file .rhosts di /usr/bin untuk memudahkan akses ke mesin yang di taklukan melalui rsh & csh. Karena itulah salah satu upaya untuk mengungkap kejahatan *cybercrime* seperti ini adalah lewat pengujian sistem yang berperan sebagai seorang detektif dan bukannya sebagai seorang user. para *hacker* dan *cracker* biasanya selangkah lebih maju dari penegak hukum, dalam melindungi diri dan menghancurkan barang bukti. Untuk itu diperlukan upaya pembuktian yang kuat untuk menegakkan hukum dalam kejahatan *hacking* dan *cracking*.

.Di Indonesia kasus *hacking* dan *cracking* sudah sangat menghawatirkan, Laporan pemantauan keamanan internet Badan Siber dan Sandi Nasional (BSSN) mencatat ada 232.447.974 serangan *cyber* yang dilakukan oleh para *hacker* dan *cracker* ke Indonesia sepanjang 2018. Dari 232,45 juta serangan ini, nyaris setengahnya atau sekitar 122.435.215 merupakan serangan malware. angka tersebut meningkat dari tahun sebelumnya sebanyak 200 juta serangan. Peningkatan serangan *cyber* oleh para *hacker* dan *cracker* ini ditengarai sebagai akibat dari semakin canggihnya serangan yang dikembangkan oleh aktor *Cybercrime*. Mengutip laporan dunia sekitar 60 hingga 70 persen sektor publik menjadi sasaran serangan *cyber*. Sementara di Indonesia, situs pemerintah dengan domain .go.id menjadi sasaran empuk serangan dan port 123 sebagai port yang paling sering diserang oleh para *hacker* dan *cracker*. Indonesia merupakan salah satu negara target srangan *cyber* terbanyak di dunia sekaligus sebagai sumber serangan terbanyak. BSSN mencatat data serangan *cyber* ini juga mencakup 2.885 serangan dari laporan publik dan 1.872 peretasan dari celah keamanan.Disamping itu, BSSN juga mencatat ada 16.939 insiden situs.[14]

Kebijakan hukum pada hakekatnya bertujuan sebagai upaya perlindungan masyarakat untuk mencapai keadilan dan kesejahteraan masyarakat. Adanya fenomena seperti yang diuraikan di atas membuat penulis tertarik untuk mengetahui lebih jauh mengenai Tinjauan hukum pidana terhadap *Hacking* Dan *Cracking* yang merupakan bagian dari Kejahatan *Cybercrime*, sehingga berdasarkan latar belakang di atas maka penulis perlu mengkaji lebih dalam

[14]CNN Indonesia, *BSSN: 232,45 Juta Serangan Siber 'Serbu' Indonesia di 2018,* https://www.cnnindonesia.com/teknologi/20190426125843-192-389855/bssn-23245-juta-serangan-siber-serbu-indonesia-di-2018 , diakses pada 24 Mei 2019

tentang permasalahan ini, yang dituangkan dalam bentuk penelitian Tesis yang berjudul: **Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (*Hacking)* Dan Menimbulkan Kerusakan (*Cracking)* Dalam Kejahatan Dunia Maya (*Cybercrime)* Menurut Perspektif Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik**

B. Rumusan Masalah

Adapun rumusan masalah dalam penelitian tesis ini adalah :

1. Bagaimana penegakan hukum pidana terhadap Pelaku *(Hacker* dan *Cracker)* dalam perspektif Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik?
2. Bagaimana aspek pembuktian terhadap *hacking* dan *cracking* menurut Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik berkaitan dengan alat bukti digital ?

C. Tujuan dan Manfaat Penelitian

1) Tujuan Penelitian

Adapun tujuan dari penelitian tesis ini adalah :

1. Untuk mendeskripsikan dan menganalisa tentang penegakan hukum pidana terhadap Pelaku *(Hacker* dan *Cracker)* dalam perspektif Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

2. Untuk mendeskripsikan dan menganalisa tentang aspek pembuktian terhadap *hacking* dan *cracking* menurut Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik berkaitan dengan alat bukti digital;

2) Manfaat Penelitian

Dalam penulisan penelitian tesis ini, setidaknya ada dua manfaat yang kiranya diharapkan akan dapat diperoleh, yaitu sebagai berikut:

Manfaat Teoritis

Dari sisi teoritis, penelitian ini memiliki tujuan untuk memberikan pengertian mengenai bagaimana tinjauan hukum pidana *hacking* dan *cracking* sebagai bentuk kejahatan *cybercrime* dalam perspektif Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, menganalisa tentang penegakan hukum pidana terhadap Pelaku *(Hacker* dan *Cracker)* menuut Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Menganalisa aspek pembuktian terhadap *hacking* dan *cracking* menurut Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik berkaitan dengan alat bukti digital. Dari tujuan – tujuan tersebut, penulisan penelitian tesis ini diharapkan dapat membuktikan bahwa *hacking* dan *cracking* sebagai bentuk tindak kejahatan *cybercrime* dapat di atasi atau tidak

dengan Undang-undang yang sudah berlaku selama ini. Dari sini dapat dilihat perlu atau tidaknya suatu pengembangan atau perubahan Undang-undang yang ada sebagai modal penegakan hukum baru yang dapat mengakomodir perkembangan masalah *cybercrime* yang setiap harinya terus berkembang.

Manfaat Praktis

Dari sisi praktis, penelitian ini diharapkan dapat memberikan masukan dalam hal uji konstitusional Undang-undang yang terkait dengan penegakan hukum terhadap tindak pidana *cybercrime* yang sudah berlaku di Indonesia dalam rangka pengembangan dan penyempurnaan peraturan peraturan perundang-undangan yang berkaitan dengan teknologi dan transaksi elektronik. Diharapkan akan terwujudnya suatu penerapan Undang-undang yang proporsional yang pada akhirnya dapat mengurangi tindak pidana *cybercrime* yang ada di Indonesia.

D. Kerangka Konseptual

Berdasarkan judul yang merupakan syarat dalam penelitian dan agar tidak terjadi kesalahpahaman dan menghindari penafsiran yang berbeda-beda dalam mengartikan istilah dalam materi penulisan penilitian tesis ini, maka penulis memberikan batasan dan memberikan defenisi dari konsep terkait dengan judul. Adapun Judul yang penulis kemukakan adalah : Tinjauan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (*Hacking)* Dan Menimbulkan Kerusakan (*Cracking)* Dalam Kejahatan Dunia Maya (*Cybercrime)* Menurut Perspektif Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi

Elektronik. penulis uraikan sebagai berikut :

1. Penegakan hukum secara konkret adalah berlakunya hukum positif dalam praktik sebagaimana seharusnya patut dipatuhi. Oleh karena itu, memberikan keadilan dalam suatu perkara berarti memutuskan hukum in concreto dalam mempertahankan dan menjamin di taatinya hukum materiil dengan menggunakan cara procedural yang ditetapkan oleh hukum formal.[15]
2. Hukum Pidana, menurut Moelyatno antara lain bahwa hukum pidana adalah bagian daripada keseluruhan hukum yang berlaku di suatu negara, yang mengadakan dasar-dasar dan aturan-aturan untuk:

   a) Menentukan perbuatan-perbuatan mana yang tidak boleh dilakukan, dilarang, dengan disertai ancaman pidana bagi siapa yang melanggarnya;
   b) Menentukan kapan dan dalam hal apa kepada mereka yang melanggar larangan dapat dikenakan pidana;
   c) Menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang melanggarnya.[16]

   Sedangkan Pompe memberikan definisi

   Bahwa hukum pidana merupakan keseluruhan peraturan yang bersifat umum yang isinya adalah larangan dan keharusan, terhadap pelanggarannya. Negara atau masyarakat hukum mengancam dengan penderitaan khusus berupa pemidanaan, penjatuhan pidana, peraturan itu juga mengatur ketentuan yang memberikan dasar penjatuhan dan penerapan pidana.[17]
3. Akses Komputer sistem komputer secara ilegal (*Hacking)* dan menimbulkan kerusakan (*cracking),* secara umum *hacking* merupakan kegiatan melakukan akses kedalam suatu sistem dengan cara yang salah

[15] Dellyana,Shant. *Konsep Penegakan Hukum*. Yogyakarta: Liberty, 2008, halaman 33
[16] Moelyatno, *Asas-asas Hukum Pidana*, Rineka Cipta, Jakarta , 2000, halaman 1.
[17] Teguh Prasetyo, *Hukum Pidana*, Raja Grafindo Persada, Jakarta,2010, halaman 22.

atau tidak sah atau ilegal, jika tindakan yang dilakukan menimbulkan kerusakan atau bersifat *destruktif* disebut *cracking.* Orang yang melakukan *hacking* disebut sebagai *hacker,* sedangkan orang yang melakukan *cracking* disebut *cracker*. Pada prakteknya *hacker* dikategorikan menjadi dua, yaitu *hacker jahat* dan *hacker baik (White hat hacker).* Namun terlepas dari hal tersebut keduanya tetap melakukan suatu akses secara ilegal.

4. Kejahatan adalah perbuatan jahat (*Strafrechtelijk misdaadsbegrip*) sebagaimana terwujud in abstracto dalam peraturan-peraturan pidana. Perbuatan yang dapat dipidana dibagi menjadi :[18]
   a) Perbuatan yang dilarang oleh Undang-undang dan;
   b) Orang yang melanggar larangan itu.
5. *Cybercrime* adalah Aktifitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan, atau disebut dengan kejahatan dunia virtual (dunia maya).[19]
6. Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah Undang-undang yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum. Undang-undang ini memiliki yurisdiksi yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-undang

[18] Barda Nawawi Arief, *Upaya Non Penal dalam Kebijakan Penanggulangan Kejahatan*, makalah disampaikan pada seminar Kriminologi VI, Semarang, tanggal 16-18 September 1991, halaman 2

[19] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw- Tinjauan Aspek Hukum Pidana*, PT Tatanusa, Jakarta, 2012, halaman 15

ini, baik yang berada di wilayah Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

7. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.[20]
8. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.[21]

E. Kerangka Teori

Teori adalah serangkaian praposisi atau keterangan yang saling berhubungan dan tersusun dalam sistem deduksi yang mengemukakan penjelasan atas suatu gejala.[22] Manfaat teori hukum dalam penelitian hukum adalah melalui teori hukum, ilmu hukum dapat mencerminkan perkembangan masyarakat. Di sini ilmu hukum tersebut membahas tentang perkembangan hukum yang berkaitan dengan perubahan-perubahan dalam masyarakatnya dan uraian ini barang tentu

---

[20] Pasal 1 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

[21] *Ibid.,*

[22] Sutan Remy Sjahdeini, *Kebebasan Berkontrak dan Perlindungan Yang Seimbang Bagi Para Pihak Dalam Perjanjian Kredit Bank Di Indonesia,* Jakarta: Pustaka Utama Grafiti, 2009, halaman 8

akan melibatkan pembicaraan mengenai struktur politiknya, pengelompokan sosialnya dan sebagainya.[23] Sementara itu, Peter Mahmud Marzuki berpendapat bahwa untuk menggali makna lebih jauh dari aturan hukum, tidak cukup dilakukan penelitian dalam ruang lingkup dogmatik hukum, melainkan lebih mendalam lagi memasuki teori hukum. Penelitian hukum dalam tataran teori diperlukan bagi mereka yang ingin mengembangkan suatu bidang kajian hukum tertentu.[24] Selain itu menurut Soerjono Soekanto, bagi suatu penelitian, teori memiliki kegunaan sebagai berikut:

1) Teori tersebut berguna untuk lebih mempertajam atau lebih mengkhususkan fakta yang hendak diselidiki atau diuji kebenarannya;
2) Teori sangat berguna di dalam mengembangkan sistem klasifikasi fakta, membina struktur konsep-konsep serta memperkembangkan definisi-definisi;
3) Teori biasanya merupakan suatu ikhtisar daripada hal-hal yang telah diketahui serta diuji kebenarannya yang menyangkut objek yang diteliti;
4) Teori memberikan kemungkinan pada prediksi fakta mendatang, oleh karena telah diketahui sebab-sebab terjadinya fakta tersebut dan mungkin faktor-faktor tersebut akan timbul lagi pada masa-masa mendatang;
5) Teori memberikan petunjuk-petunjuk terhadap kekurangan-kekurangan pada pengetahuan peneliti. [25]

Kerangka teori yang digunakan dalam penelitian tesis ini adalah Teori Penegakan hukum dan teori pembuktian.

1. Teori Penegakan Hukum

Negara didirikan demi kepentingan umum dan hukum adalah sarana utama untuk merealisasikan tujuan tersebut. Suatu masyarakat dianggap baik, bila kepentingan umum (*bonum commune*) diperhatikan, baik oleh para penguasa

[23] Disadur dari Satjipto Rahardjo, *Ilmu Hukum*, Bandung: PT. Citra Aditya Bakti, 2014, halaman 9

[24] Disadur dari Peter Mahmud Marzuki, *Penelitian Hukum*, Cet. Ke-6, Jakarta: Kencana, 2010, halaman 72-73.

[25] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Cet. Ke-3, Jakarta: Penerbit Universitas Indonesia (UI Press), 2006, halaman 121

maupun oleh para warga negara.[26] Kalau dikatakan bahwa kepentingan umum menjadi bisa diwujudkan melalui hukum, diandaikan pula bahwa kepentingan-kepentingan lain sudah diperhatikan secukupnya oleh manusia pribadi, yakni kepentingan individual.[27] Namun hal ini berarti juga bahwa hukum yang menjamin kepentingan umum tidak boleh merugikan kepentingan individual, tetapi harus melindunginya. Hukum yang memelihara kepentingan umum menyangkut juga semua sarana publik bagi berjalannya kehidupan manusia beradab. Pada prinsipnya kepentingan umum secara de fakto dilindungi oleh negara dan hukum.[28]

Penegakan hukum merupakan suatu usaha untuk mewujudkan ide-ide keadilan, kepastian hukum dan kemanfaatan sosial menjadi kenyataan. Jadi penegakan hukum pada hakikatnya adalah proses perwujudan ide-ide. Penegakan hukum adalah proses dilakukannya upaya tegaknya atau berfungsinya norma-norma hukum secara nyata sebagai pedoman pelaku dalam lalu lintas atau hubungan-hubungan hukum dalam kehidupan bermasyarakat dan bernegara. Penegakan hukum merupakan usaha untuk mewujudkan ide-ide dan konsepkonsep hukum yang diharapakan rakyat menjadi kenyataan. Penegakan hukum merupakan suatu proses yang melibatkan banyak hal.[29]

Menurut Soerjono Soekanto, ada lima unsur yang mempengaruhi penegakan hukum yaitu:

---

[26] Roscou Pound, *Pengantar Filsafat Hukum*, Jakarta : Bhratara Karya Aksara, 1982, halaman 27.

[27] Lili Rasjidi, *Dasar-Dasar Filsafat Hukum*, Bandung : Citra Aditya Bakti, 1996, halaman 84.

[28] Theo Huijbers, *Filsafat Hukum Dalam Lintasan Sejarah*, Jogyakarta:Kanisius,1982, halaman 287.

[29] Dellyana,Shant. Konsep Penegakan Hukum. Yogyakarta: Liberty, 1988, halaman 32

a. Faktor hukumnya sendiri hanya dibatasi oleh undang-undang saja;
b. Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukumnya.;
c. Faktor sarana atau fasilitas yang mendukung penegakan hukum;
d. Faktor masyarakat yaitu lingkungan dimana hukum tersebut berlaku atau diterapkan; [30]

Lebih jauh Soerjono Soekanto, mengatakan bahwa penegakan hukum adalah kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan dalam kaidah-kaidah mantap dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir. Untuk menciptakan, memelihara dan mempertahankan kedamaian pergaulan hidup.[31]

Penegakan hukum pidana adalah penerapan hukum pidana secara konkrit oleh aparat penegak hukum. Dengan kata lain, penegakan hukum pidana merupakan pelaksaan dari peraturan-peraturan pidana. Dengan demikian, penegakan hukum merupakan suatu sistem yang menyangkut penyerasian antara nilai dengan kaidah serta perilaku nyata manusia. Kaidah-kaidah tersebut kemudian menjadi pedoman atau patokan bagi perilaku atau tindakan yang dianggap pantas atau seharusnya. Perilaku atau sikap tindak itu bertujuan untuk menciptakan, memelihara, dan mempertahankan kedamaian. Menurut Moeljatno menguraikan berdasarkan dari pengertian istilah hukum pidana yang mengatakan bahwa penegakan hukum adalah bagian dari keseluruhan hukum yang berlaku disuatu Negara yang mengadakan unsur unsur dan aturan-aturan, yaitu:

a. Menentukan perbuatan-perbuatan yang tidak boleh di lakukan dengan di sertai ancaman atau sanksi berupa pidana tertentu bagi barang siapa yang melanggar larangan tersebut.

---

[30] Soerjono Soekanto, *Faktor – Faktor yang Mempengaruhi Penegakan Hukum*, Edisi Revisi, Jakarta: RajaGrafindo Persada, 2012, halaman 5.

[31] *Ibid*,. halaman 35

b. Menentukan dan dalam hal apa kepada mereka yang melanggar laranganlarangan itu dapat dikenakan atau dijatuhi pidana sebagaimana yang telah diancamkan.
c. Menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila orang yang disangkakan telah melanggar larangan tersebut.[32]

Indonesia telah memiliki Undang-undang yang khusus mengatur tentang teknologi informasi yang semakin berkembang yang mengubah baik perilaku masyarakat maupun peradaban manusia secara global, hubungan dunia menjadi tanpa batas (*borderless*). Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) diharapkan mampu untuk menghadang kejahatan dan menegakan hukum dibidang teknologi informasi saat ini. Untuk dapat melihat upaya penegakannya dapat digunakan teori Lawrence M. Friedman, yaitu bahwa faktor – faktor yang mempengaruhi penegakan hukum meliputi struktur hukum *(legal structure),* subtansi hukum *(legal subtance)* dan budaya hukum *(legal culture).* Sistem hukum terdiri tiga unsur tersebut dapat dijabarkan sebagai berikut :

a. Struktur, mencangkup instusi – instusi penegakan hukum termasuk penegakan hukumnya ;
b. Subtansi, mencakup aturan – aturan hukum baik yang tertulis maupun yang tidak tertulis, termasuk putusan pengadilan ;
c. Budaya Hukum, mencakup opini – opini, kebiasaan-kebiasaan, cara berfikir dan cara bertindak, baik dari penegak hukum maupun dari warga masyarakatnya.[33]

Sistem hukum mempunyai struktur, kerangka atau rangkanya, bagian yang tetap bertahan, bagian yang memberi semacam bentuk dan batasan terhadap

[32] Moeljatno, *Asas-Asas hukum Pidana* Jakarta: Bina Aksara, 2008, halaman 23
[33] Lawrence M. Friedman, *Hukum Amerika, Sebuah Pengantar, Terjemahan dari Wishnu Basuki*, Jakarta : Tatanusa, 2001 halaman 190.

keseluruhan . Sedangkan maksud dari subtansi adalah aturan, norma, dan pola perilaku nyata manusia yang berada dalam sistem itu. Penekanannya terletak pada hukum yang hidup, bukan hanya pada aturan kitab hukum (*law books*). Selanjutnya, hal ini membawa kita kepada komponen ketiga yaitu budaya hukum, yaitu sikap manusia terhadap hukum dan sistem hukum; kepercayaan, nilai , pemikiran dan harapannya. Dengan kata lain budaya hukum adalah suasana pikiran sosial dan kekuatan sosial yang menentukan bagaimana hukum digunakan, dihindari atau disalah gunakan. Tanpa budaya hukum sistem hukum itu sendiri tidak akan berdaya.[34]

Terkait dengan *hacking* dan *cracking* terhadap jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global/Internet dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual (*Cyberspace*). Internet merupakan media yang bersifat lintas batas wilayah dan negara, sehingga apabila terjadi tindak pidana akan sulit untuk menentukan *locus delictienya*, karena akan bersinggungan dan melibatkan kepentingan negara lain. Hal ini menjadi kendala pula dalam penegakan hukumnya akan tetapi tidak bisa dibiarkan berlarut – larut dan harus segera dicarikan alternatif pemecahannya.

2. Teori Pembuktian

Dalam pembuktian tindak pidana *hacking* dan *cracking* ini tidak bisa dilakukan dengan cara yang bersifat konvensional. Dalam ha1 pembuktiannya harus menggunakan cara-cara yang di luar dari kebisaaan pembuktian selama ini.

[34] *Ibid*., halaman 8

Untuk membahas pembuktian pada tindak pidana *hacking* dan *cracking* tersebut penulis akan menggunakan teori dan/atau doktrin yaitu

a) Teori

Menurut M.Yahya Harahap, pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa.[35] Dalam sistem pembuktian terdapat macam-macam sistem atau teori pembuktian, sistem pembuktian tersebut adalah:

1) Pembuktian Berdasarkan Keyakinan Hakim Belaka (*Conviction in Time*) yakni Suatu sistem pembuktian yang bersifat subjektif, yakni untuk menentukan bersalah atau tidaknya terdakwa hanya berdasarkan keyakinan hakim semata. Putusan hakim tidak didasarkan kepada alatalat bukti yang diatur oleh undang undang, hakim hanya mengikuti hati nuraninya saja. Keyakinan hakim dapat diperoleh dan disimpulkan hakim dari alat-alat bukti yang diperiksanya dalam sidang pengadilan. Hakim dapat juga mengabaikan hasil pemeriksaan alat-alat bukti itu, dan langsung menarik keyakinan dari keterangan atau pengakuan terdakwa. Sistem ini seolah-olah menyerahkan sepenuhnya nasib terdakwa kepada keyakinan hakim sepenuhnya. Keyakinan hakimlah menentukan wujud kebenaran sejati dalam sistem pembuktian ini.[36]
2) Sistem Pembuktian Berdasarkan Undang-undang Secara Positif (*Positief*

[35] M. Yahya Harahap, *Pembahasan Pemasalahan Dan Penerapan KUHAP Pemeriksaan Sidang Pengadilan Banding Kasasi dan Peninjauan Kembali*, Jakarta, Sinar Grafika, 2006, halaman 273

[36] *Ibid.,* halaman 277

Wettelijk Bewijstheorie) yakni Suatu sistem pembuktian yang berkembang pada zaman pertengahan yang ditujukan untuk menentukan bersalah atau tidaknya terdakwa harus berpedoman pada prinsip pembuktian dengan alat-alat bukti yang ditentukan undang-undang.[37] Sistem ini berbanding terbalik dengan *Conviction in Time*, dimana keyakinan hakim disampingkan dalam sistem ini. Menurut sistem ini, undang-undang menetapkan secara limitatif alat-alat bukti yang mana yang boleh dipakai hakim. Jika alat-alat bukti tersebut telah dipakai secara sah seperti yang ditetapkan oleh undang-undang, maka hakim harus menetapkan keadaan sah terbukti, meskipun hakim ternyata berkeyakinan bahwa yang harus dianggap terbukti itu tidak benar.

3) Sistem Pembuktian Berdasarkan Keyakinan Hakim atas Alasan yang Logis (*La Conviction Raisonee*), Menurut sistem pembuktian ini, hakim memegang peranan yang penting disini. Hakim baru dapat menghukum seorang terdakwa apabila ia telah meyakini bahwa perbuatan yang bersangkutan terbukti kebenarannya. Keyakinan tersebut harus disertai dengan alasan-alasan yang berdasarkan atas suatu rangkaian pemikiran (logika). Hakim wajib menguraikan dan menjelaskan alasan-alasan yang menjadi dasar keyakinannya atas kesalahan terdakwa.[38] Sistem pembuktian ini mengakui adanya alat bukti tertentu tetapi tidak ditetapkan secara limitatif oleh undang-undang.

4) Sistem Pembuktian Menurut Undang-undang Secara Negatif (*Negatief*

[37] Edmon Makarim, *Kompilasi Hukum Telematika*, Jakarta, Rajagrafindo Persada, 2003, halaman. 421

[38] *Ibid*., halaman. 422

Wettelijk Bewijstheorie), Sistem ini merupakan penggabungan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian berdasarkan keyakinan hakim semata. Hasil penggabungan ini dapat dirumuskan : "salah tidaknya seorang terdakwa ditentukan oleh hakim yang didasarkan kepada cara dan dengan alat-alat bukti yang sah menurut undang-undang". "Sistem pembuktian menurut undangundang secara negatif ini merupakan suatu keseimbangan antara sistem yang saling bertolak belakang secara ekstrim".[39] Dalam sistem atau teori pembuktian yang berdasarkan undang undang secara negatif (n*egatief wettelijk bewijstheorie*) ini, pemidanaan didasarkan kepada pembuktian yang berganda (*dubbel engrondslag*, menurut D. Simmons), yaitu pada peraturan perundang undangan dan pada keyakinan hakim, dan menurut undang-undang, dasar keyakinan hakim itu bersumber pada peraturan undang-undang.[40]

b) Doktrin Undang-undang

Menurut Soejono Soekanto, yang diartikan dengan Undang-undang dalam arti materiel adalah peraturan tertulis yang berlaku umum dan dibuat oleh penguasa pusat maupun daerah yang sah. Dengan demikian maka Undang-undang dalam materil (selanjutnya disebut Undang-undang) mencangkup:[41] 1). Peraturan Pusat yang berlaku untuk semua warga Negara atau suatu golngan tertentu saja maupun berlaku umum disebagian wilayah Negara. 2). Peraturan setempat yang

[39] Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP Jilid I dan II*, Jakarta, Pustaka Kartini, 1988 dan 1993, halaman. 799

[40] Andi Hamzah, Hukum Acara Pidana Indonesia, Jakarta, Sinar Grafika, 2005, halaman. 250

[41] Soerjono Soekanto, *Op. cit.,* halaman 11

hanya berlaku di suatu tempat atau daerah saja.

Kitab Undang-undang Hukum Pidana (KUHP) telah memberikan pengaturan yang jelas mengenai batas-batas berlakunya aturan perundang-Undang hukum pidana. Hal ini diatur dalam Bab I buku ke Satu KUHP yang terdiri dari Sembilan pasal mulai dari pasal 1 sampai pasal 9. Dalam pasal 1 KUHP diatur mengenai batas-batas berlakunya hukum pidana menurut waktu atau saat terjadinya perbuatan. Sedangkan pasal 2 samapai dengan pasal 9 KUHP diatur mengenai batas-batas berlakunya perundang-Undangan hukum pidana menurut tempat terjadinya perbuatan.[42] Berkenaan dengan pengaturan di atas, Moelyatno mengemukakan bahwa dari sudut Negara ada dua kemungkinan pendirian, yaitu:

> Pertama, perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang terjadi di wilayah Negara, baik yang di lakukan oleh warga Negaranya sendiri maupun oleh orang asing (asas teritorial). Kedua, perundang- Undangan hukum pidana berlaku bagi semua perbuatan pidana yang dilakukan oleh warga negara dimana saja, juga di luar wilayah Negara (asas personal). Juga dinamakan Prins'ip Nasional yang aktif.[43]

Menurut Joseph Raz, bahwa ciri khas yang paling umurn dan penting dari hukum adalah hukum bersifat normatif, terlembaga, dan memaksa. Hukum menjadi normatif pada saat ia melayani untuk memberi petunjuk bagi perilaku manusia. Terlembaga ketika penerapan aturannya dilakukan atau diatur oleh lembaga-lembaga. Bersifat memaksa manakala ketaatan kepadanya dan dalam aplikasinya pada akhirnya dijamin secara internal melalui penggunaan kekuatan

---

[42] Didik M. Arief Mansur, Cyber Law Aspek Hukum Teknologi Informasi, Bandung: Aditama ,2009, hlm. 40.

[43] Moelyatno,*asas-asas hukum pidana,Op. cit.,* halaman 38

pemaksa.[44]

Undang-undang memiliki cara untuk mencapai suatu tujuan yang memang sudah di desain terhadapnya, sehingga Undang-undang tersebut akan efektif dalam penerapannya. Supaya tujuan itu tercapai maka terdapat berbagai asas untuk menunjang tercapainya tujuan tersebut, asas yang sesuai dengan pembuktian pada tindak pidana *hacking* dan *cracking* adalah asas Undang-undang yang bersifat khusus mengenyampingkan Undang-undang yang bersifat umum, apa bila perbuatannya sama.

Arti dari asas tersebut adalah bahwa terhadap peristiwa khusus wajib diperlakukan Undang-undang yang menyebutkan peristiwa itu, walaupun bagi peristiwa khusus tersebut dapat pula yang lebih luas ataupun lebih umum, yang dapat juga mencakup peristiwa khusus tersebut.[45]

Selain itu pasal yang dapat menjadi dasar adalah pasal 184 KUHAP, yang berbunyi :

Alat Bukti Sah Menurut Pasal 1 84 (1) KUHAP:[46]

1) Keterangan Saksi;
2) Keterangan Ahli;
3) Surat;
4) Petunjuk;
5) Keterangan Terdakwa.

F. Metodologi Penelitian

Istilah "metode penelitian" terdiri dari dua kata, yakni kata "metode" dan kata "penelitian". Kata "metode" menurut etimologi-nya (asal kata)

---

[44]Aroma Elmina Martha, *Perempuan Dan Kekerasan Dalam Rumah Tangga Di Indonesia Dan Malaysia*, Yogyakarta,FH.UI1 PRESS, 2012, halaman. 22

[45] Soerjono Soekanto, *Op. cit.,* halaman 12

[46] KUHAP pasal 184

merupakan gabungan dari dua kata, yaitu "*meta*" yang berarti menuju, melalui, mengikuti, sesudah dan "*hodos*" yang berarti jalan, cara, arah, sehingga pengertian dari metode menurut *etimologi*-nya adalah jalan menuju. Jadi pengertian metode adalah kegiatan ilmiah yang berkaitan dengan suatu cara kerja (sistematis) untuk memahami suatu subjek atau objek penelitian, sebagai upaya untuk menemukan jawaban yang dapat dipertanggung jawabkan secara ilmiah dan termasuk keabsahannya.[47]

Sedangkan kata "penelitian" berasal dari kata dalam bahasa Inggris yakni *research, re* yang berarti kembali dan *search* yang berarti pencarian, sehingga pengertian penelitian menurut *etimologi*-nya adalah pencarian kembali. Menurut Tuckman, penelitian adalah suatu usaha yang sistematis untuk menemukan jawaban ilmiah terhadap suatu masalah. Sistematis artinya mengikuti prosedur atau langkah-langkah tertentu. Jawaban ilmiah adalah rumusan pengetahuan, generaliasi, baik berupa teori, prinsip baik yang bersifat abstrak maupun konkret yang dirumuskan melalui alat- primernya, yaitu empiris dan analisis. Penelitian itu sendiri bekerja atas dasar asumsi, teknik dan metode.[48] Oleh karena itu, metode penelitian adalah rangkaian langkah sistematis untuk memecahkan suatu rangkaian sebab akibat dan menemukan jawaban ilmiah terhadap suatu permasalahan.

---

[47] Ruslan, Rosdy. Metode Penelitian Publik. PT Raja Grafindo Persada, Surabaya, 2003, halaman 24

[48] Jonathan, Sarwono. Metode Penelitian Kuantitatif dan Kualitatif, Graha Ilmu, Yogyakarta, 2006. halaman 15

1. Spesifikasi Penelitian

Penelitian yang dilakukan oleh penulis adalah penelitian deskriptif dengan pendekatan bersifat yuridis normatif, terutama ditujukan untuk mengkaji kaidah/asas hukum yang terkait dengan masalah tindak pidana *hacking* dan *cracking* berdasarkan ketentuan peraturan perundang-undangan terkait tindak pidana *cybercrime* di indonesia. Penelitian hukum normatif artinya penelitian yang bertitik berat terhadap data yang didapatkan dari aturan atau norma hukum positif dan menjadi bahan acuan utama dalam penelitian ini.[49] Sedangkan menurut Peter Machmud Marzuki, penelitian hukum adalah suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi.[50] Oleh karena itu, penelitian hukum merupakan suatu penelitian di dalam kerangka *know-how* di dalam hukum.[51]

2. Tehnik Pendekatan

Sesuai dengan tujuan yang akan dicapai, maka metodologi dalam desain penelitian tesis ini menggunakan tiga macam pendekatan, yakni Pendekatan Perundang-undangan (*Statute Approach*), Pendekatan Konseptual (*Conceptual Approach*), serta Pendekatan Kasus (*Case Approach*).[52] Pendekatan Perundang-undangan (*Statute Approach*) merupakan pendekatan yang dilakukan dengan menelaah semua peraturan perundang-undangan mengenai kejahatan *cybercrime*.

---

[49] Soerjono Soekanto, *Op.Cit*, halaman 51

[50] Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta 2009, halaman 35

[51] *Ibid.* halaman 41.

[52] Peter Mahmud Marzuki, *Op. cit*., halaman 29 -36.

Pendekatan demikian merupakan cara untuk menemukan konsistensi pengaturan hukum pidana terkait *hacking* dan *cracking* sebagai bentuk kejahatan *cybercrime* . Pendekatan Konseptual dilakukan dengan harapan ditemukan konsep-konsep baru seiring dengan diamika dan perubahan sosial yang terjadi untuk menjawab isu hukum penelitian. Sedangkan pendekatan kasus dilakukan untuk menjaring preseden berupa putusan pengadilan yang berkaitan dengan pembuktian kasus *hacking* dan *cracking*, sebagai dasar pertimbangan majelis hakim dalam putusannya. Berdasarkan tiga pendekatan tersebut diharapkan dapat diperoleh kedalaman analisa baik dari aspek norma yang sedang berlaku, konsep-konsep yang terus berkembang hingga putusan pengadilan sehingga hasil penelitian ini nanti dapat melahirkan preskripsi yang menyeluruh.

3. Jenis dan Sumber Data

Data yang digunakan dalam penelitian ini adalah data pustaka (*library research*). penelitian ini adalah penelitian kepustakaan yang dilakukan dengan metode mencari, mengumpulkan, dan mengolah data dari bahan-bahan kepustakaan yang relevan dan penting.[53] Oleh karena itu, penelitian ini menggunakan bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

a. Bahan Hukum Primer

Merupakan bahan hukum yang bersifat *aoturitatif* artinya mempunyai otoritas. Bahan-bahan hukum primer terdiri dari peraturan perundang-

[53] Franmastaka Bramantya Saktiarditto, *Metode Penelitian Metris*, 2009 dari http://cuplis.net/2009/03/metode-penelitian-metris/ diunduh pada tanggal 30 April 2019

undangan, catatan-catatan resmi.[54] Dalam penelitian ini, Penulis mengunakan terdiri dari norma dasar, peraturan perundang-undangan, yurisprudensi maupun traktat.

b. Bahan Hukum Sekunder

Yaitu bahan hukum yang menjelaskan bahan hukum primer, seperti data yang diperoleh dari data dokumen-dokumen resmi, buku-buku yang berhubungan dengan objek penelitian, hasil penelitian dalam bentuk laporan, skripsi, tesis, disertasi dan sebagainya.[55]

c. Bahan Hukum Tersier

Bahan hukum tersier yaitu hukum yang memberikan penjelasan mengenai bahan hukum sekunder. Seperti kamus, ensiklopedia, indeks kumulatif, bahan yang berasal dari bahan internet.[56]

4. Tehnik Pengumpulan data

Prosedur tehnik pengumpulan data dalam penelitian ini terdiri dari pengumpulan bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier yang dilakukan melalui tahapan sebagai berikut : **pertama**, melakukan sistematisasi produk hukum dalam bentuk peraturan perundang-undangan mengenai hukum yang mengatur *cybercrime* berikut hukum hukum pidana dan hukum acara pidana. **Kedua**, melakukan klasifikasi peraturan perundang-undangan yang yang berkaitan dengan isu hukum yang harus dijawab. Klasisifikasi ini dilakukan atas dasar pendekatan hirarkhis, materi muatan dan

[54] Soerjono Soekarto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Rajawali Pers, Jakarta, 2011, halaman 62.

[55] Peter Mahmud Marzuki, *Op. cit*,. halaman 181.

[56] Abdulkhadir Muhammad, *Hukum Dan Penelitian Hukum*, Citra Aditia Bakti, Bandung, 2004, halaman 125.

lembaga pembentuk peraturan perundang-undangan. Tujuannya untuk memudahkan proses mengkaji dan menganalisis kesesuaian antara permasalahan dalam penelitian inidengan asas-asas hukum pidana.

5. Tehnik Analisis Data

Setelah bahan hukum terkumpul, langkah selanjutnya adalah melakukan analisis terhadap bahan hukum primer dan bahan hukum sekunder. Analisis hukum, menurut Kelsen[57] adalah "…suatu analisis tentang struktur hukum positif, yang dilakukan seeksak mungkin, suatu analsis yang bebas dari semua pendapat etik atau politik mengenai nilai" Analisis hukum hendaklah ketat dan bersih dari pertimbangan-pertimbangan non hukum. Konsekuensinya konstruksi hukum hendaklah tidak dicemari oleh ilmu politik, sosiologi, sejarah, dan pembicaraan tentang etika.

Dalam penelitian tesis ini analisis terhadap bahan hukum yang ada dilakukan secara *Preskriptif Analitis*, yang bertujuan untuk menghasilkan preskripsi mengenai apa yang seharusnya sebagai esensi dalam penelitian hukum yang berpegang pada karater ilmu hukum sebagai ilmu terapan. Hasil kajian dan analisis dengan menggunakan logika hukum, penafsiran hukum, argumentasi hukum serta asas-asas hukum yang pada gilirannya menghasilkan kesimpulan sebagai jawaban atas isu hukum yang harus dijawab.

[57] Jimly Asshiddiqie dan M.Ali Safa'at, *Dari Hans Kelsen Tentang Hukum, Sekretariat Jenderal dan Kepaniteraan Mahkamah Konstitusi RI*, Jakarta, 2006, halaman 43.

G. Sistematika Penulisan

Sistematika disajikan untuk mempermudah pembaca dalam memahami materi yang akan dibahas selanjutnya dalam tesis ini. Dengan adanya sistematika ini diharapkan pembaca dapat mengetahui secara garis besar tesis ini. Tesis ini dibagi kedalam 5 bab, yang akan diuraikan sebagai berikut :

Bab Satu Pendahuluan, Bab ini akan menguraikan Bab ini menguraikan mengenai latar belakang permasalahan, pernyataan masalah, perumusan masalah, tujuan dan manfaat penelitian, kerangka teori, kerangka konsep, Metodologi penelitian yang digunakan dalam penelitian ini serta sistematika penulisan.

Bab Kedua, Bab ini akan menguraikan umum mengenai tinjauan umum tentang kejahatan dunia maya (*Cybercrime)*, dimulai dari Defenisi Kejahatan Dunia Maya *(Cybercrime),* Jenis-Jenis Kejahatan *Cybercrime,* Unsur-unsur Tindak Pidana dalam *Cybercrime,* Pengaturan Hukum *Cybercrime* di Indonesia serta ruang lingkup *Cybercrime*

Bab Ketiga, Bab ini akan membahas tentang Akses Sistem Komputer Secara Ilegal (*Hacking)* Dan Menimbulkan Kerusakan (*Cracking)* Dalam Hukum Pidana Di Indonesia, nantinya akan dijlaskan mulai dari Defenisi *Hacking* dan *Cracking,* Tahapan-tahapan dalam Melakukan *Hacking* dan *Cracking,* Konstruksi *Hacking* dan *Cracking* Sebagai Kejahatan *Cybercrime,* Pengaturan Hukum Pidana Terhadap *Hacking* dan *Cracking* baik menurut KUHP, serta Aspek Yurisdiksi dalam penegakan hukum terhadap pelaku kejahatan *Hacking* dan *Cracking*.

Bab Keempat Bab ini akan membahas tentang penegakan hukum terhadap Pelaku *(Hacker* dan *Cracker)* dan Aspek pembuktian berkaitan dengan alat bukti

digital terhadap kejahatan *hacking* dan *cracking* menurut Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Bab Kelima Penutup, dimana subbabnya akan berisi kesimpulan dan saran.

BAB II

TINJAUAN UMUM TENTANG KEJAHATAN DUNIA MAYA (*CYBERCRIME)*

A. Defenisi Kejahatan Dunia Maya *(Cybercrime)*

Sebelum mengurai pengertian kejahatan dunia maya (*cybercrime*) secara terperinci, maka terlebih dahulu akan dijelaskan "induk" kejahatan dunia maya (*cybercrime*) yaitu *cyber space*. *Cyber space* dipandang sebagai sebuah dunia komunikasi berbasis komputer. Dalam hal ini, *cyber space* di anggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan internet. Realitas baru ini dalam kenyantaannya terbentuk melalui jaringan komputer yang menghubungkan antarnegara atau antar benua yang berbasis protokol. Hal ini berarti, dalam sistem kerjanya dapatlah dikatakan bahwa internet (*cyberspace*) telah mengubah jarak dan waktu menjadi tidak terbatas. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda.[58]

Dalam perkembangan selanjutnya kehadiran teknologi canggih komputer dengan jaringan internet telah membawa manfaat besar bagi manusia. Pemanfaatannya tidak saja dalam pemerintahan, dunia swasta/perusahaan, akan tetapi sudah menjangkau pada seluruh sektor kehidupan termasuk segala keperluan rumah tangga (pribadi). Internet telah mampu membuka cakrawala baru

[58] Maskun, *Kejahatan Siber Cyber Crime, Kencana*, Jakarta, 2013, halaman. 46

dalam kehidupan manusia baik dalam konteks sarana komunikasi dan informasi yang menjanjikan menembus batas-batas negara maupun penyebaran dan pertukaran ilmu pengetahuan dan gagasan di kalangan ilmuan di seluruh dunia.[59] Akan tetapi, kemajuan teknologi informasi (internet) dan segala bentuk manfaat di dalamnya membawa konsekuensi negatif tersendiri di mana semakin mudahnya para penjahat untuk melakukan aksinya yang semakin merisaukan masyarakat. Penyalahgunaan yang terjadi dalam internet (*cyber space*) atau dalam kata lain Kejahatan Dunia Maya *(cybercrime)*.

Kejahatan Dunia Maya *(cybercrime)* merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional *(street crime)*. *cybercrime* muncul bersamaan dengan lahirnya revolusi teknologi informasi. Pada masa awalnya, *cybercrime* didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para ahli belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan penggunaan istilah tindak pidana untuk kejahatan komputer dalam bahasa Inggris pun masih belum seragam. Beberapa ahli menggunakan istilah *computer misuse, computer abuse, computer fraud, computer related crime, computer assistend crime, atau computer crime*. Namun para ahli pada waktu itu, pada umumnya lebih menerima pemakaian istilah *computer crime* oleh karena dianggap lebih luas dan bias dipergunakan dalam hubungan internasional.

---

[59] Widyopramono Hadi Widjojo, *Cybercrimes dan Pencegahannya*, jurnal Hukum Teknologi, Fakultas Hukum Universitas Indonesia, 2005, halaman. 7

Secara etimologi *cybercrime* berasal dari dua rangkaian kata, yaitu *cyber* dan *crime*. Menurut Kamus Bahasa Inggris-Indonesia *cyber* berarti maya, sedangkan *crime* diartikan dengan kejahatan.[60] Menurut *Dictionary of Contemporary English, crime* adalah *an offence which is punishable by law* (suatu kejahatan yang dihukum oleh hukum), *illegal activity in general* (kegiatan ilegal pada umumnya), atau *a bad, immoral, or dishonourable act* (tidak terhormat, tidak bermoral, atau tindakan yang buruk).[61] Secara kebahasaan *cybercrime* semakna dengan "kejahatan dunia maya" atau "kejahatan mayantara".

Menurut beberapa literatur, *cybercrime* sering diidentikkan dengan *computer crime*. *The US Department of Justice* memberikan pengertian computer crime sebagai *"any illegal act requiring knowledge of computer for it's perpetration, investigation, or prosecution",* artinya "setiap perbuatan melanggar hukum yang memerlukan pengetahuan tentang komputer untuk menangani, menyelidiki dan menuntutnya".[62]

Sementara pengertian lainya diberikan oleh *Organization of European Community Development*, yaitu: *"any illegal, unethical or unauthorized behaviour relating to the automatic processing and/or the transmission of data"*, artinya "setiap prilaku ilegal, tidak pantas, tidak mempunyai kewenangan yang berhubungan dengan pengolahan data dan/atau pengiriman data".[63]

---

[60] John M. Echols dan Hassan Shadily, *Kamus Inggris-Indonesia Cet. XXV*; Jakarta:Gramedia Pustaka Utama, 2003, halaman. 155.

[61] Longman Group, *Longman dictionary of Contemporary English* Ed. VIII England, 1998, halama. 155

[62] Tim Andi Yogykarta dan Wahana Komputer Semarang. *Kamus Lengkap Dunia Komputer* Edisi I; Yogyakarta: Andi Yogyakarta dan Wahana Komputer Semarang, 2002, halaman. 419

[63] *Ibid.,*

Menurut laporan kongres PBB X/2000 dinyatakan *cybercrime* atau *computer-related crime*, mencakup keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan pada komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer.[64]

Kepolisian Republik Indonesia dalam hal ini unit *Cybercrime*, menggunakan parameter berdasarkan dokumen kongres PBB tentang *The Prevention Of Crime and Treatment Of Offlenderes di Havana*, Cuba pada tahun 1999 dan di Wina, Austria Tahun 2000. Convetion on Cybercrime tidak menganggap terminologi *"cybercrime"* sebagai kata yang urgen untuk didefinisikan. Hanya ada empat kata yang didefinisikan dalam konvensi tersebut, yaitu *"computer system"* , *"computer data", "service data"* dan *"traffic data*".[65] Secara umum kejahatan yang berbasis pada teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu computer misuse, computer abuse, computer fraud, computer- related crime, computer-assisted crime, atau computer crime.

Muladi dalam bukunya yang ditulis bersama Barda Nawawi Arief, "Bunga Rampai Hukum Pidana" memandang *cybercrime* dengan pendekatan *computer crime* (kejahatan komputer).[66] Namun demikian, *cybercrime* sesungguhnya

---

[64] Barda Nawawi Arief, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan* Cet. I; Bandung, PT Citra Aditya Bakti, 2005, halaman. 136. Lihat juga dalam Dokumen Kongres PBB X, A/CONF.187/L.10, 16-4-2000, halaman. 1-2 dan dokumen A/CONF.187/15,19-7-2000, halaman. 26:

[65] Dokumen Kongres PBB tentang *The Prevention Of Crime and Treatment Of Offlenderes* di Havana, Cuba pada tahun 1999

[66] Agus Rahardjo. *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bakti, 2002, Halaman. 227

berbeda dengan *computer crime*. Meskipun demikian, ada upaya untuk memperluas pengertian komputer agar dapat melingkupi segala kejahatan di internet dengan peralatan apapun, seperti pengertian komputer dalam *The Proposed West Virginia Computer Crimes Ac*t;

> *an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or type-setter, a portable hand-held calculator, or other similar device"*. (peralatan pemerosesan data listrik, magnetik, optik, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau *tipe-setter*, sebuah kalkulator tangan atau peralatan serupa lainnya).[67]

Dengan demikian, pendapat yang mengidentikkan *cybercrime* dengan *computer crime* dapat dipahami dengan menggunakan pendekatan pemaknaan komputer yang diperluas seperti pengertian tersebut di atas. Pengertian yang membedakan antara *cybercrime* dengan *computer crime* diajukan oleh Nazaru Abdul Manap sebagai berikut:

> *Defined broadly, "computer crime" could reasonably include a wide variety of criminal offences, activities or issues. It also known as a crime committed using a computer as tool and it involves direct contact between the criminal and the computer. For instance, a dishonest bank clerk who unauthorisedly transfers a costumer's money to dormant account for his own interest or a person without permission has obtained acces to other person's computer directly to download information, which in the first place, are confidential. Tehe situations require direct access by the hacker to the victim's computer. There is no Internet line involved. Or only limited networking used such as the local area network (LAN). Whereas, cyber-crimes are crimes commited virtually through internet online. This means*

[67] John R. Vacca, *Computer and Information Security Handbook,* Burlington:Morgan Kaufmann Publishers, 2009, halaman. 266

> *that the crimes committed could extend to other countries, which is beyond the Malaysian jurisdiction. Anyway, it causes no harm to refe computer crimes as cybercrimes or vice versa, since they have same impact in law. (*Maksudnya adalah didefinisikan secara luas, kejahatan komputer dapat meliputi lingkup luas bermacam-macam pelanggaran, aktivitas atau isu kriminal. Ini dikenal dengan kejahatan yang dilakukan dengan komputer sebagai alat dan melibatkan hubungan langsung antara kriminal dan komputer. Contoh sebuah pegawai bank yang tidak jujur yang secara tidak sah mentransfer uang konsumen kepada akun-tidur untuk kepentingannya sendiri atau orang yang tanpa izin memperoleh akses terhadap komputer orang lain secara langsung untuk men-download informasi, yang pertama kali adalah terpercaya. Situasi ini membutuhkan akses langsung oleh hacker kepada komputer korban. Tidak ada saluran internet yang terlibat atau hanya menggunakan jaringan terbatas seperti LAN (*local area network*).Di mana kejahatan *cyber* adalah kejahatan yang dilakukan secara *virtual* (maya) melalui internet *online*. Ini berarti bahwa kejahatan yang dilakukan dapat berkembang ke negara lain yang berada di luar yurisdiksi Malaysia. Meskipun demikian, ini tidak dapat menyebabkan kejahatan computer sebagaimana kejahatan cyber atau sebaliknya, ketika mereka mempunyai dampak sama di dalam hukum).[68]

Muladi dalam bukunya yang ditulis bersama Barda Nawawi Arief, "Bunga Rampai Hukum Pidana" memandang *cybercrime* dengan pendekatan *computer crime* (kejahatan komputer). Namun demikian, *cybercrime* sebenarnya berbeda dengan *computer crime*.[69]*Cybercrime* di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer, akan tetapi melibatkan teknologi telekomunikasi di dalam pengoperasiannya.

Hal ini juga dikemukakan oleh Agus Raharjo, bahwa istilah *cybercrime* sampai saat ini belum ada kesepakatan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cyber crime* dengan *computer crime*.[70]

---

[68] Agus Rahardjo. *Op.cit,* Halaman. 227
[69] *Ibid.*
[70] *Ibid.*

Barda Nawawi Arief menggunakan istilah "tindak pidana mayantara" untuk menyebut *cybercrime*. Barda Nawawi Arief mengatakan, dengan istilah "tindak pidana mayantara" dimaksudkan identik dengan tindak pidana di ruang cyber (*cyber space*) atau yang biasa juga dikenal dengan istilah "*cybercrime*".[71]

Indra Safitri yang mengemukakan pandangannya bahwa *cybercrime* adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah sistem teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[72]

Dari berbagai pengertian *computer crime* di atas, dapat dikemukakan rumusan definisi *cybercrime* yang tidak jauh substansinya dari pengertian yang disebutkan oleh para ahli tersebut. Hal ini dimaksudkan sebagai bentuk ketegasan dalam menarik benang merah dari perbedaan yang ada, sehingga pengertian *cyber crime* dapat tergambar secara jelas dan mudah dipahami

Maka, dapat disimpulkan bahwa *cybercrime* merupakan suatu kejahatan baru yang berhubungan dengan Teknologi informasi atau dunia maya (*cyber space*), yang mana kejahatannya dilakukan melalui sistem elektronik dengan jaringan internet yang berbasis komputer dan komputer dijadikan sebagai sarana atau alat untuk melakukan kejahatan.

---

[71] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Bandung: Citra Aditya Bakti, 2003. Halaman 239

[72] Maskun, *Kejahatan Siber Cyber Crime*, Kencana,Jakarta, 2013, halaman 47-48

B. Jenis-Jenis Kejahatan *Cybercrime*

Seperti halnya defenisi dari *cybercrime,* jenis-jenis *cybercrime* juga berbeda-beda, karena setiap ahli memiliki pendapat yang berbeda-beda, selain itu juga belum ada kesepakatan yang seragam mengenai pengertian *cybercrime* membuat banyaknya perbedaan tersebut.

Nazura Abdul Manap berpendapat , kejahatan *cybercrime* dapat dibedakan ke dalam 3 (tiga) kelompok kategori, yaitu:[73]

pertama, *cybercrimes against property* (kejahatan maya terhadap hak milik). Misalnya, pencurian informasi properti, dan pelayanan, *fraud* atau *cheating, forgery*, dan *mischief*. Tiga yang terakhir menyangkut perilaku penipuan, pemaksaan, penjambretan, dan yang sejenis.

Kedua, *cyber crimes against Persons* (kejahatan maya terhadap orang). Kejahatan ini meliputi pornografi, *cyber harassment* (pelecehan, seperti pelecehan seksual, terhadap seseorang melalui dunia maya), *cyber stalking* (mengejar-ngejar seseorang atau mengikuti terus-menerus sehingga mengganggu orang yang dikejar- kejar), dan *cyber tresspass* ini dibagi lagi ke dalam spam e-mail, web *hacking*, dan *breaking to PC*. Intinya, masuk ke dalam wilayah pribadi seseorang tanpa izin.

Ketiga, adalah *cyber terorism*. Terorisme maya (*cyber terorism*) berdimensi luas, tetapi semua menyangkut isu-isu terorisme, mulai dari sekadar pemanfaatan jasa internet untuk berkomunikasi melakukan tindak kejahatan

[73] Sutanto, Hermawan Sulistiyo, dan Tjuk Sugiarto, *Cyber Crime - Motif dan Penindakan* Jakarta: Pensil, 2005, halaman 21

terorisme, hingga pemanfaatan langsung jaringan maya untuk melakukan teror publik.[74]

Menurut *Convention on Cybercrime*, tindak pidana yang dapat digolongkan sebagai cybercrime diatur dalam pasal 2-5, adapun jenis tindak pidana tersebut adalah :

a) Illegal Access[75]

Illegal access melingkupi pelanggaran dasar dari ancaman-ancaman yang berbahaya dari serangan terhadap keamanan data dan sistem komputer. Perlindungan terhadap pelanggaran *illegal access* ini merupakan gambaran dari kepentingan organisasi atau kelompok dan orang-orang yang ingin mengatur, menjalankan dan mengendalikan sistem mereka berjalan tanpa ada ganguan dan hambatan.

Pasal ini merupakan ketentuan pertama yang mengatur mengenai masalah *cybercrime*. Sebagai contoh dari kejahatan ini adalah *hacking, cracking* atau *computer trespassing*. Gangguan jenis ini memberikan akses kepada pelaku terhadap data-data penting (termasuk password atau informasi sistem) dan rahasia-rahasia, yang mungkin digunakan untuk membeli barang dengan menggunakan informasi kartu kredit milik orang lain atau mendorong pelaku untuk melakukan bentuk pelanggaran berkenaan dengan komputer yang lebih berbahaya, seperti pemalsuan atau penipuan dengan komputer.[76]

---

[74] Sebagaimana dikutip oleh Sutanto Hermawan Sulistiyo, dan Tjuk Sugiarto (Ed). Lihat dalam: *Ibid*, halaman. 14.

[75] Council of Europe, *Explanatory Report To The Convention on Cybercrime* (ETS No 185), Budapest, 23.XI.2001, pasal 44 Halaman 9

[76] Mike Keyser, "*The Council of Europe Convention on Cybercrime*", Journal of Transnational Law and Policy, volume 12, 2003, halaman. 300,

b) Illegal Interception[77]

Menyatakan tidak sah tindakan pencegatan atau menahan tanpa hak bentuk pemindahan data komputer yang dilakukan secara pribadi yang dilakukan melalui *faximile, email,* atau pemindahan *file*. Tujuan dari pasal ini adalah perlindungan atas hak atas kebebasan dalam komunikasi data. Pelanggaran ini hanya ditujukan terhadap pemindahan pribadi dari data komputer. Pengertian interception secara teknis dijleaskan dalam *Council of Europe, Explanatory Report To The Convention on Cybercrime* yaitu:

> "*Interception by techincal means relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or undirectly through the use of electronic eavesdropping or taping devices.Interception may also involving recording*."
> Intersepsi secara teknis berarti berhubungan dengan mendengarkan, memantau atau mengawasi konten komunikasi, untuk pengadaan konten data baik secara langsung, melalui akses dan penggunaan sistem komputer, atau secara tidak langsung melalui penggunaan perangkat penyadap atau rekaman elektronik. Intersepsi juga dapat melibatkan perekaman/[78]

Salah satu bagian dari pelanggaran yang dimaksud dari ketentuan pasal ini adalah melakukan penahanan komunikasi atau menghambat proses komunikasi dengan menggunakan perangkat elektronik untuk mendengarkan pembicaraan orang lain atau menggunakan peralatan untuk menyadap komunikasi. Klasifikasi ini hanya berlaku pada komunikasi data komputer yang dilakukan secara pribadi, klasifikasi ketentuan ini mengacu pada sifat pemindahan dan sifat dari data yang dipindahkan. Komunikasi yang terjadi dapat melalui hubungan dari komputer ke

---

https://pdfs.semanticscholar.org/593e/f4735e7ac0e01a2168cdbd72167a514854cb.pdf, Akses pada tanggal 26 Juli 2019

[77] *Ibid,*. Halaman 10

[78] *Ibid*

printer, antara dua komputer atau dari orang ke komputer itu sendiri (seperti mengetik dengan keyboard).[79]

c) Data Interception

Ketentuan pengerusakan data menjadi tindak pidana bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program komputer sebagaimana dengan benda-benda berwujud. Sebagai contoh adalah memasukan kode-kode jahat (*malicous codes*), *Viruses*, dan *Trojan Horse* ke suatu sistem komputer merupakan pelangagaran menurut ketentuan pasal ini.

Berdasarkan Pasal 4 ayat 1 merupakan tindak pidana apabila dilakukan dengan terencana tindakan merusak, menghapus, memperburuk, mengubah atau mengembangkan suatu data komputer tanpa hak.[80] Ketentuan yang diatur dalam pasal ini berusaha untuk memberi jaminan bahwa data yang dikirimkan melaui jaringan internet atau pemindahan data yang dilakukan melaui suatu jaringan adalah sama dengan data yang dikirimkan oleh si pengirim. Kepentingan perlindungan hukum dalam pasal ini adalah keutuhan dan berfungsi sebagaimana mestinya penggunaan data komputer yang tersimpan atau program- program komputer.[81]

d) System Interference

Dalam Pasal 5 konvensi ini disebutkan bahwa system interference ditetapkan sebagai pelanggaran pidana apabila *"... when committed intentionally, the serious hindering without right of the functioning of a computer system…",*

[79] Keyser, *.loc cit*., Halaman 301.
[80] *Ibid.,* Halaman 302
[81] *Council of Europe, Op.Cit* Halaman 11

harus dilakukan dengan memasukkan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer.[82]

Pengganguan terhadap sistem dijadikan sebagai tindak pidana bertujuan untuk *mencegah "...the serious hindering without right of the functioning of a computer system..."*[83]

Sebagai contoh adalah serangan *denial-of-service (DOS)* yang dilakukan dengan teknik *hacking*, pembuatan kode jahat seperti virus. Contoh tersebut dapat memperlambat penggunaan sistem komputer yang mengakibatkan pengguna tidak dapat mengakses suatu *website.*

Menurut NCIS Inggris, sebagaimana dikutip oleh Ade Maman Suherman, menyatakan bahwa manifestasi dari tindak pidana *cybercrime* muncul dalam berbagai macam atau varian sebagai berikut:[84]

1. ***Recreational Hackers***

Kejahatan ini dilakukan oleh netter tingkat pemula untuk sekadar mencoba kekuranghandalan sistem sekuritas suatu perusahaan.

2. ***Crackers atau criminal minded hackers***

Pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan *finansial*, sabotase, dan penghancuran data. Sebagai contoh, pada tahun 1994 Citibank AS kebobolan senilai 400.000 dolar oleh cracker dari Rusia yang akhirnya dijatuhi hukuman penjara selama tiga tahun serta harus mengembalikan sejumlah uang tersebut. Tipe kejahatan ini dapat terjadi dengan bantuan orang

---

[82] *Ibid,.* Halaman 12

[83] Keyser, *.loc cit.*, hal 303

[84] NCIS Inggris dalam Ade Maman Suherman, *Aspek Hukum Dalam Ekonomi Global* Jakarta: Ghalia Indonesia, 2002, halaman.168-171

dalam, biasanya staf yang sakit hati atau datang dari kompetitor dalam bisnis sejenis.

3. Political Hackers

Aktivitas politik atau lebih populer dengan sebutan *hactivist* melakukan perusakan terhadap ratusan situs web untuk mengkampanyekan program-programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendeskriditkan lawannya. Usaha tersebut pernah dilakukan secara aktif dan konsisten dalam usaha untuk kampanye anti – Indonesia dalam masalah Timor Timor yang dipelopori oleh Ramos Horta. Situs Deplu (departemen luar negeri) sempat mendapat serangan yang diduga keras dari kelompok anti integrasi.

4. Denial of Service Attack

Serangan denial of service attack atau oleh FBI dikenal dengan istilah *"unprecedented"* tujuannya adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna yang legitimate. Taktik yang digunkan adalah dengan mengirim atau membanjiri situs web dengan data yang tidak perlu. Pemilik situs web menderita kerugian karena untuk mengendalikan atau mengontrol kembali situs web memakan waktu yang tidak sedikit.

5. Insiders atau Internal Hackers

Insider hackers ini bisa dilakukan oleh orang dalam perusahaan sendiri. Modus operandinya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan. Departemen Perdagangan dan Industri Inggris mengumumkan bahwa pada tahun 1998 ada banyak perusahaan-perusahaan yang telah menderita kerugian senilai 1,5 miliar poundsterling.

6. Viruses

Program penggangu *(malicious)* dengan penyebaran virus dewasa ini dapat menular melalui aplikasi internet. Sebelumnya, pola penularan virus hanya melalui floppy disk. Virus bisa bersembunyi dalam *file* dan *ter-download* oleh user bahkan bisa menyebar melalui kiriman *e-mail*. Seperti halnya dunia kedokteran, dunia komputer telah menciptakan jurus antivirus, seperti *melissa* 1999 atau *lovebug* 2000, tetapi masih belum bisa berbuat banyak.

7. Piracy Pembajakan softwere

Merupakan trend dewasa ini. Pihak produsen softwere dapat kehilangan profit karena karyanya dapat dibajak melalui down load dari internet dan di kopi ke dalam CD-Rom yang selanjutnya diperbanyak secara ilegal atau tanpa seizin penciptanya.

8. Fraud

Fraud adalah sejenis manipulasi informasi keuangan dengan tujuan mengeruk keuntungan sebesar-besarnya. Sebagai contoh, harga tukar saham yang menyesatkan melalui rumor. Situs lelang fiktif dengan mengeruk uang masuk dari para peserta lelang dan barangnya tidak dikirim bahkan identitas pelakunya tidak dapat dilacak.

9. Gambling

Perjudian di dunia *cyber* yang berskala global sulit dijerat dengan hukum nasional suatu negara. Dari kegiatan gambling dapat diputar kembali di negara yang merupakan *tax heaven*, seperti *Cayman Island* yang merupakan surga bagi *money laundring*. Bahkan Indonesia negara yang sering dijadikan sebagai tujuan

money laundring yang uangnya diperoleh dari hasil kejahatan berskala internasional.

10. Pornography and Paeddophilia

Dunia *cyber* selain mendatangkan berbagai kemudahan dengan mengatasi kendala ruang dan waktu, juga telah melahirkan dunia pornografi yang mengkhawatirkan berbagai kalangan. Melalui *news group, chat rooms* mengekploitasi pornografi anak-anak di bawah umur.

11. Cyber - Stalking

Cyber-Stalking adalah segala bentuk kiriman e-mail yang tidak dikehendaki oleh user atau junk e-mail yang sering memadati folder serta tidak jarang dengan pemaksaan meskipun *e-mail* "sampah" tidak dikehendaki oleh user. Bahkan sering juga pelaku/pengirim secara paksa memperoleh identitas personal secara detail calon para korbannya.

12. Hate Sites

Situs ini sering dipergunakan untuk saling menyerang dan melontarkan komentar-komentar yang tidak sopan dan vulgar yang dikelola oleh para ekstrimis. Penyerangan terhadap lawan atau *opponent* sering mengangkat isu rasial, perang program dan promosi kebijakan atau suatu pandangan.

13. Criminal Communications

NCIS telah mendeteksi bahwa internet telah dijadikan sebagai alat handal dan modern untuk malakukan komunikasi antar gangster, anggota sindikat obat bius, dan komunikasi antar hooligan di dunia sepak bola.

Menurut *Global Internet Policy Initiative* (GIPI), ada empat kategori dari pelanggaran yang dikategorikan sebagai cybercrime, yaitu:[85]

1) *Data iterception;*
2) *Data interference;*
3) *System interference;*
4) *Illegal access.*

Pembagian oleh GIPI ini pada dasarnya sejalan dengan dengan jenis-jenis *cybercrime* yang diatur di dalam *Convention on Cybercrime*. Jenis-jenis *cybercrime* yang telah dipaparkan telah menjadi bentuk yang dikenal oleh masyarakat seiring dengan perkembangan teknologi informasi. Berdasarkan jenis-jenis *cybercrime* tersebut dapat dilakukan pembagian atas tiga kategori, yaitu:

1) *Cyberpiracy;*
2) *Cybertersspass;*
3) *Cybervandalism*

Dari sekian banyak pembagian jenis-jenis *cybercrime,* dapat ditarik gambaran secara umum bahwa yang termasuk ke dalam jenis-jenis *cybercrime* berdasarkan modus operandinya adalah :

1. *Unauthorized Access to Computer System and Service*

   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya *(Hacking)*. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan

[85] 53 Gobal Internet Policy Initiative, *Trust and Security in Cyberspace :The Legal and Policy Framework forAdressing Cybercrime*, 2005, Halaman 3 https://www.internetpolicy.net/cybercrime/20050900cybercrime.pdf, Akses 25 Juli 2019

maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.

2. *Illegal Contents*

   Merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

3. *Data Forgery*

   Merupakan kejahatan dengan memalsukan data pada dokumen dokumen penting yang tersimpan sebagai scripless document melalui Internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah- olah terjadi "salah ketik", yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

4. *Cyber Espionage*

   Merupakan kejahatan yang memanfaatkan jaringan Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki

sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (data base) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer).

5. *Cyber Sabotage and Extortion*

   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6. *Offense against Intellectual Property*

   Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh, peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7. *Infringements of Privacy*

   Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat

merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

C. Unsur-unsur Tindak Pidana dalam *Cybercrime*

Berdasarkan asas yang berlaku dalam hukum pidana, maka tidak ada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam Peraturan Perundang-Undangan yang telah ada sebelum perbuatan itu dilakukan (Pasal 1 Ayat (1) KUHP).[86] Sekalipun perkembangan mutakhir dalam hukum pidana menunjukkan bahwa asas hukum tersebut tidak lagi diterapkan secara rigid atau kaku, tetapi asas hukum tersebut sampai sekarang tetap dipertahankan sebagai asas yang sangat fundamental dalam hukum pidana sekalipun dengan berbagai modifikasi dan pengembangan.[87] Dengan demikian seseorang hanya dapat dipersalahkan melakukan tindak pidana apabila orang tersebut melakukan perbuatan yang telah dirumuskan dalam ketentuan undang-undang sebagai tindak pidana. Sejauh mana seseorang melakukan perbuatan yang telah dirumuskan dalam undang-undang sebagai tindak pidana dapat dipersalahkan melakukan tindak pidana.

Lazimnya Jawaban normatif yang diberikan oleh hukum pidana berdasarkan asas legalitas seperti tersebut di atas adalah, bahwa seseorang hanya dapat dipersalahkan sebagai telah melakukan tindak pidana apabila orang tersebut oleh hakim telah dinyatakan terbukti bersalah dengan memenuhi unsur-unsur dari tindak pidana yang bersangkutan, seperti yang dirumuskan di dalam undang-undang. Dengan kata lain dapat dikemukakan, bahwa seseorang tidak dapat

[86] Moeljatno, *Asas-Asas hukum Pidana*,. *Op. Cit*. 23

[87] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Bandung, Citra Aditya Bakti, 1996, halaman. 88

dipersalahkan melakukan tindak pidana apabila salah satu unsur tindak pidana yang didakwakan kepada orang tersebut tidak dapat dibuktikan. Sebab tidak terpenuhinya salah satu unsur tindak pidana tersebut membawa konsekuensi dakwaan atas tindak pidana tersebut tidak terbukti. Sekalipun demikian, batasan normatif tersebut dalam perkembangannya mengalami pergeseran, dimana sangat dimungkinkan orang tetap dapat dipersalahkan melakukan suatu tindak pidana berdasarkan nilai-nilai yang hidup dalam masyarakat sekalipun perbuatan tersebut tidak secara tegas diatur dalam perangkat normatif atau undang-undang.

Bertolak dari berbagai tuntutan normatif tersebut, pemahaman terhadap unsur-unsur tindak pidana merupakan kebutuhan yang sangat mendasar berkaitan dengan penerapan hukum pidana materiil. Secara umum unsur-unsur tindak pidana dapat dibedakan ke dalam dua macam yaitu:

1. **Unsur Obyektif, yaitu unsur yang terdapat di luar pelaku (dader) yang dapat berupa:**

a. Perbuatan, baik dalam arti berbuat maupun dalam arti tidak berbuat. Contoh unsur obyektif yang berupa "perbuatan" yaitu perbuatan-perbuatan yang dilarang dan diancam oleh undang-undang. Perbuatan-perbuatan tersebut dapat disebut antara lain perbuatan-perbuatan yang dirumuskan di dalam Pasal 242, 263, 362 KUHP. Di dalam ketentuan Pasal 362 KUHP misalnya, unsur obyektif yang berupa "perbuatan" dan sekaligus merupakan perbuatan yang dilarang dan diancam oleh undang-undang adalah perbuatan mengambil.
b. Akibat, yang menjadi syarat mutlak dalam tindak pidana materiil. Contoh unsur obyektif yang berupa suatu "akibat" adalah akibat-akibat yang dilarang

dan diancam oleh undang-undang dan sekaligus merupakan syarat mutlak dalam tindak pidana antara lain akibat-akibat sebagaimana dimaksudkan dalam ketentuan Pasal 351, 338 KUHP. Dalam ketentuan Pasal 338 KUHP misalnya, unsur obyektif yang berupa "akibat" yang dilarang dan diancam dengan undang-undang adalah akibat yang berupa matinya orang.

c. Keadaan atau masalah-masalah tertentu yang dilarang dan diancam dalam undang-undang. Contoh unsur obyektif yang berupa suatu "keadaan" yang dilarang dan diancam oleh undang-undang adalah keadaan sebagaimana dimaksud dalam ketentuan Pasal 160, 281 KUHP. Dalam ketentuan Pasal 282 KUHP misalnya, unsur obyektif yang berupa "keadaan" adalah ditempat umum.[88]

2. Unsur Subyektif, yaitu unsur yang terdapat dalam diri si pelaku (dader) yang berupa:

a. Hal yang dapat dipertanggungjawabkannya seseorang terhadap perbuatan yang telah dilakukan (kemampaun bertanggung jawab).

b. Kesalahan atau *schuld*

Berkaitan dengan masalah kemampuan bertanggung jawab di atas, persoalannya adalah kapan seseorang dapat dikatakan mampu bertanggung jawab? seseorang dapat dikatakan mampu bertanggung jawab apabila dalam diri orang itu memenuhi tiga syarat, yaitu:

[88] P.A.F. Lamintang dan Djisman Samosir, *op. cit*. Lihat juga, Suharto R.M., *Hukum Pidana Materiil Unsur-unsur Obyektif sebagai Dasar Dakwaan* , Jakarta, Sinar Grafika, 1991, halaman. 1.

1) Keadaan jiwa orang itu adalah sedemikian rupa, sehingga ia dapat mengerti akan nilai perbuatannya dan karena juga mengerti akan nilai dari akibat perbuatannya itu.
2) Keadaan jiwa orang itu sedemikian rupa, sehingga ia dapat menentukan kehendaknya terhadap perbuatan yang ia lakukan.
3) Orang itu harus sadar perbuatan mana yang dilarang dan perbuatan mana yang tidak dilarang oleh undang-undang. [89]

Sementara itu berkaitan dengan persoalan kemampuan bertanggung jawab ini pembentuk KUHP berpendirian, bahwa setiap orang dianggap mampu bertanggung jawab.

Konsekuensi dari pendirian ini adalah, bahwa masalah kemampuan bertanggung jawab ini tidak perlu dibuktikan adanya di pengadilan kecuali apabila terdapat keragu-raguan terhadap unsur tersebut. Bertolak dari pendirian pembentuk KUHP di atas, dapat dimengerti di dalam KUHP sendiri tidak ada penjelasan tentang apa yang dimaksud dengan kemampuan bertanggung jawab. KUHP hanya memberikan rumusan secara negatif atas kemampuan bertanggung jawab ini terdapat di dalam ketentuan Pasal 44 KUHP yang menyatakan kapan seseorang tidak dapat dipertanggungjawabkan atas perbuatannya. Pasal KUHP menyatakan, bahwa seseorang tidak dapat dipertanggungjawabkan atas perbuatannya karena sebab:

[89] *Ibid.,*

a. Jiwanya cacat dalam tumbuhnya

Keadaan ini menunjuk pada suatu keadaan dimana jiwa seseorang itu tidak tumbuh dengan sempurna. Termasuk dalam kondisi ini adalah idiot, imbisil, bisu tulis sejak lahir, dan lain-lain.[90]

b. Jiwanya terganggu karena suatu penyakit

Dalam hal ini jiwa seseorang itu pada mulanya berada dalam keadaan sehat, tetapi kemudian dihinggapi oleh suatu penyakit. Termasuk dalam kondisi ini misalnya maniak, histeria, melankolia, gila dan lain-lain

Unsur subyektif kedua adalah unsur "kesalahan" atau schuld. Sebagaimana diketahui, bahwa kesalahan atau schuld dalam hukum pidana dibedakan menjadi dua bentuk, yaitu:

a) *Dolus* atau *opzet* atau kesengajaan.

b) *Culpa* atau ketidaksengajaan.

Di antara dua unsur subyektif tersebut di atas yang sangat penting berkaitan dengan pembicaraan tentang unsur-unsur tindak pidana adalah kesalahan dalam bentuk "kesengajaan" atau *opzet*. Hal ini disebabkan hampir semua tindak pidana mengandung unsur *opzet*. Sebagaimana dalam azas-azas hukum pidana umum di dunia nyata hukum pidana mengatur banyak hal tentang kepentingan publik di atas kepentingan pribadi. Hukum pidana mengatur sanksi bagi pelaku tindak pidana dengan hukum badan. Sama halnya di dalam dunia *cyber* (mayantara) unsur-unsur yang ada dalam tindak pidana di bidang ini tidak

[90] R. Soesilo, *Kitab Undang-undang Hukum Pidana (KUHP) Serta Komentar-komentamya Lengkap Pasal Demi Pasal* Bogor, Politeia, Bogor, 1998, halaman. 8.

berbeda, karena yang membedakan hanya modus operandi dan di dalam dunia yang berbeda yakni dunia *cyber*. Unsur-unsur tindak pidana dibagi atas 2 (dua):

1) Unsur subyektif, artinya unsur subyektif suatu tindak pidana pelaku dengan maksud atau memang sudah dari awal bermaksud melakukan suatu tindakan melawan hukum. Jadi yang menjadi titik tolak dari jenis kejahatan ini adalah dari pelaku tindak pidana.
2) Unsur obyektif, artinya obyek tindak pidana tersebut bukan setatus miliknya, dan dilakukan melawan hak atau tanpa dan hak mengambil alih, menguasai dan menimbulkan hak atas obyek tersebut

Jadi, jelas ada dua unsur yang saling mengikat antara unsur obyektif satu dengan yang lain berhubungan dalam dunia *cyber* dapat kita konstruksikan kondisi sebagai berikut:

- ✓ Unsur subyektif yakni : - *wetwede dat* (yang diketahui)
  - *Opzettelijk* (dengan sengaja)
- ✓ Unsur obyektif yakni : - *ontrekken* (menjauhkan)
  - *Vergegen* (menyembunyikan)
  - *Eaning goed* (suatu benda)

Karena sifat dari internet juga mengutamakan kerahasiaan baik yang menyangkut rahasia dagang atau informasi rahasia lainnya yang berpotensi dapat disebarkan kepada pihak ketiga tanpa izin pemilik informasi, maka prinsip-prinsip umum di dalam KUHP tidak dapat sepenuhnya dipakaikan dalam menjerat pelaku sebagai bentuk pertanggungjawaban secara pidana.

Dasar pemikiran lain adalah urgensi penggunaan hukum pidana dalam penanggulangan *cybercrime*, jika kriminalisasi suatu perbuatan pidana. Menurut Prof. Nigel Weker, ada beberapa hal yang diperhatikan antara lain:

a. Kerugian suatu tindak pidana harus jelas termasuk korbannya harus jelas.
b. Penegakan hukum (*law an forcemant*) harus mendapatkan dukungan masyarakat luas dan dilakukan secara efektif.
c. Kerugian yang timbul karena pemindahan ini harus lebih kecil dai padacakibat tindak pidana.[91]

Unsur melawan hukum (Pasal 1365 KUHPerdata) adalah unsur sangat penting dalam kejahatan *cyber*, sudah barang tentu akan menimbulkan kerugian ekonomis pihak lain akibat dari perbuatannya.

D. Pengaturan Hukum *Cybercrime* di Indonesia

Cybercrime adalah suatu istilah yang digunakan oleh para ahli hukum khususnya hukum *cyber* (*cyber law*).[92] Lebih lanjut dinyatakan bahwa *cybercrime* adalah suatu kejahatan baru yang sangat berbeda dengan dua jenis kejahatan yang sudah ada sebelumnya, *blue collar crime* (arti harfiahnya kejahatan kerah biru) dan *white collar crime* (arti harfiahnya kejahatan kerah putih). *Blue collar crime* adalah kejahatan konvensional seperti pencurian, pembunuhan dan lain-lain. Sedangkan *white collar crime*, menurut Jo Ann Miller, umumnya dibagi ke dalam

---

[91] Robintan Sulaiman, *Cyber Crimes (Perspektif E-Commerce Crime)* Cet. I, Jakarta, Universitas Pelita Harapan, 2002, halaman. 90-92

[92] Istilah "Hukum *cyber*" diartikan sebagai padanan kata dari "*Cyber Law*" , yang saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah Hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara. Penjelasan tersebut dapat dilihat dalam Ahmad M. Ramli, *Cyber Law dan HAKI-dalam Sistem Hukum Indonesia* Cet. I, Bandung, PT Refika Aditama, 2004, halaman. 1

4 (empat) jenis, yaitu: kejahatan korporasi, kejahatan birokrasi, malpraktek dan kejahatan individu.[93]

Sementara itu, *cybercrime* memiliki ciri khas tersendiri. Para pelaku pada umumnya anak-anak muda yang menguasai teknologi informasi. Dalam berbagai kasus yang telah terungkap dan pelakunya tertangkap, sebagian di antaranya terbukti bahwa pelakunya adalah anak-anak muda, bahkan masih remaja. Di antara kasus- kasus besar tersebut, ada di antaranya yang merupakan hasil dari sekedar tindakan "iseng" atau coba-coba".[94]

Ahmad M. Ramli menyatakan,teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif untuk melakukan perbuatan melawan hukum.[95]

Pernyataan Ahmad M. Ramli di atas menjadi alasan pembenaran terhadap suatu adagium "di mana ada masyarakat, di situ ada kejahatan".[96] Dua sisi inilah yang menjadi realitas potret kehidupan yang sebenarnya. Konsep yang dibangun secara ideal selalu melahirkan realitas lain yang menyimpang dari konsep ideal tersebut, yakni tindakan melawan hukum (kejahatan dan pelanggaran). Adagium lain seperti *"ubi societis, ibi ius"* (di mana ada masyarakat di situ ada hukum) juga ikut membenarkan, bahwa kriminalitas yang terjadi sejatinya adalah cermin riil kehidupan masyarakat, bahwa ada tali-temali antara hukum masyarakat, dan

---

[93] Sutantu, Hermawan Sulistiyo dan Tjuk Sugiarto dalam Sutarman, *Cyber Crime: Modus Operandi dan Penanggulangannya* Cet. I, Yogyakarta, LaksBang Pressindo, 2007, halaman 31.

[94] *Ibid.,* halaman 32

[95] Achmad Sodiki dalam AbdulWahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* Cet. I, Bandung, Refika Aditama, 2005, halaman. vii.

[96] *Ibid.,*

kriminalitas. Masyarakat membutuhkan hukum, karena masyarakat mencita-citakan kehidupan yang damai, tertib, nyaman atau agar hak-haknya tidak diganggu oleh yang lain.

Oleh karena itu, upaya penanggulangan kejahatan sesungguhnya merupakan usaha yang terus menerus dan terus berkesinambungan. Semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi, muncul berbagai jenis kejahatan berdimensi baru, yang termasuk didalamnya *cybercrime*. Sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi ketertiban masyarakat. Akan tetapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab terhadap dampak negatif yang timbul dari kejahatan. Hal ini dikarenakan teknologi yang membawa perubahan dalam masyarakat berkembang begitu pesat, sementara hukum pidana merupakan produk sejarah tertentu berjalan dengan logika sejarah yang menaunginya walaupun dalam batas tertentu mempuntyai prediktabilitas atas perkembangan masyarakat. Menjawab tuntutan dan tantangan komunikasi global melalui rung maya (*cyber space*), undang-undang yang diharapkan *ius konstituendum*, yakni perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.

Saat ini, Indonesia telah memiliki undang-undang khusus *(cyber law)* yang mengatur mengenai *cybercrime*, undang-undang yang dimaksud adalah Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik. Meskipun demikian demikian undang-undang tersebut belum berjalan secara optimal. Hal ini terjadi karena adanya pasal-pasal yang memiliki multi tafsir. Sehingga dampak dari pasal tersebut menjerat pelaku yang bukan sasaran undang- undang.

Selain undang-undang *cybercrime* tersebut, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

1. Kitab Undang-undang Hukum Pidana (KUHP)

Dalam upaya penanganan kasus-kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cybercrime* antara lain:

a) Dalam Pasal 362 dan Pasal 378 KUHP yang dikenakan untuk kasus Pencurian kartu kredit (*carding)* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang direkam melalui *software card generator* di internet untuk melakukan transaksi di situs jual beli online (*e-commerce)*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin

mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi

b) Dalam Pasal 378 KUHP dapat dikenakan untuk penipuan dengan modus operandi seolah-olah menawarkan dan menjual suatu barang dengan memasang iklan di sebuah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut hanya *fiktif*. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

c) Dalam Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban.

d) Dalam Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan *e-mail* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan *e-mail* ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.

e) Dalam Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di internet dengan penyelenggara dari Indonesia.

f) Dalam Pasal 282 KUHP dapat dikenakan terhadap pelaku penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak para pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negeri dimana pornografi yang menampilkan adegan dewasa bukan merupakan hal yang ilegal.

g) Dalam Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto/video pribadi seseorang yang vulgar/ berbau porno di internet, misalnya kasus Ariel-Luna Maya atau Ariel-Cut Tari.

h) Dalam Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

2. Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan

Dengan dikeluarkannya Undang-undang Nomor 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya *Compact Disk - Read Only Memory (CD - ROM),* dan *Write - Once - Read - Many (WORM)*, yang diatur dalam Pasal 12 undang-undang tersebut sebagai alat bukti yang sah.

3. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-undang Nomor 36 Tahun 1999 karena Undang-undang ini merupakan undang-undang pertama mengatur tentang tindak pidana

cyber.Penyelenggaraan telekomunikasi di Indonesia mengalami perubahan yang sangat signifikan dengan adanya Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang disahkan dan diundangkan pada tanggal 8 September 1999. Undang-undang ini lahir sebagai konsekuensi dari adanya perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi yang memerlukan penataan dan pengaturan kembali penyelenggaraan telekomunikasi nasional.[97] Reformasi di bidang industri telekomunikasi termasuk liberalisasi industri, ketentuan bagi penyelenggaraan baru dan peningkatan struktur kompetitif industri.

Di dalam Undang-undang Nomor 36 Tahun 1999 yang pertama kali diatur adalah tentang siapa saja yang berhak menyelenggarakan telekomunikasi sesuai dengan peruntukannya. Pihak-pihak yang melakukan kegiatan telekomunikasi dikenal dengan istilah penyelenggaraan telekomunikasi dapat merupakan perseorangan, korperasi, badan usaha milik daerah, badan usaha swasta, instansi pemerintah dan instansi pertahanan keamanan negara. Undang-undang ini merupakan amandemen dari Undang-undang sebelumnya yaitu Undang-undang Nomor 3 Tahun 1989 tentang Telekomunikasi dan menjadi undang-undang pertama yang memasukkan *cybercrime* sebagai salah satu pelanggaran di dalam bidang telekomunikasi walaupun undang-undang ini masih tidak tegas menyebutnya. Sehingga sulit diterapkan dan dikenakan terhadap pelakunya. Kebijakan hukum yang terkait dengan masalah pengaturan mengenai *cybercrime*

[97] Sutan Remy Sjahdeini, *Kebebasan Berkontrak dan Perlindungan Yang Seimbang Bagi Para Pihak Dalam Perjanjian Kredit Bank Di Indonesia*, Jakarta, Pustaka Utama Grafiti, 2009, Halaman 40

pada Undang-undang ini diatur dalam Pasal 21, Pasal 38 dan Pasal 40 yang berbunyi:[98]

> Pasal 21: Penyelenggaraan telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, keamanan, atau ketertiban umum.
> Pasal 38:"Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi."
> Pasal 40 : " Setiap Orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun."

Di dalam Pasal 21 Undang-undang Telekomunikasi tersebut tidak mengatur tindak kejahatan dan hal ini tidak diatur pula di dalam ketentuan pidana di dalam Bab VII Ketentuan Pidana Pasal 47 sampai dengan Pasal 57. Ketentuan terhadap Pasal 21 berarti hanya merupakan pelanggaran yang berdasarkan ketentuan Bab VI Pasal 46 sanksinya berupa pencabutan izin. Akibat ringannya sanksi hukum tersebut pornografi dan tindakan pengasutan melalui media telekomunikasi sering terjadi dan dilakukan oleh penyelenggaraan telekomunikasi.

Berdasarkan penjelasan Pasal 38 perbuatan yang dapat digolongkan sebagai perbuatan yang dapat menyebabkan gangguan telekomunikasi adalah:[99]

a) Tindakan fisik yang menimbulkan kerusakan suatu jaringan telekomunikasi sehingga jaringan tersebut tidak dapat berfungsi sebagaimana mestinya;
b) Tindakan fisik yang mengakibatkan hubungan telekomunikasi tidak berjalan sebagaimana mestinya;

---

[98] Undang-undang tentang Telekomunikasi , UU Nomor 36 Tahun 1999, LN Tahun 1999 Nomor 154, TLN Nomor 3881. Pasal 21, Pasal 38 dan Pasal 40

[99] *Ibid.*, Penjelasan Pasal 38

c) Penggunaaan alat telekomunikasi yang tidak sesuai dengan persyaratan teknis yang berlaku;
d) Penggunaan alat telekomunikasi yang bekerja dengan gelombang radio yang tidak sebagaimana mestinya sehingga menimbulkan gangguan terhadap penyelenggaraan telekomunikasi Iainnya; atau
e) Penggunaan alat bukan telekomunikasi yang tidak sebagaimana mestinya sehingga menimbulkan pengaruh teknis yang tidak dikehendaki suatu penyelenggaraan telekomunikasi.

Sedangkan menurut penjelasan Pasal 40 yang dimaksud dengan *Cyber spy* adalah: "kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah." Dari penjelasan pasal 38 dan pasal 40 tersebut dapat kita simpulkan bahwa yang diatur di dalam Undang-undang ini adalah salah satu perbuatan yang termasuk dalam kategori tindak pidana *cyber* yaitu *illegal interception*.[100]

4. Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta

Menurut Pasal 1 angka (8) Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-

[100] Cybercrime Convention,Op.Cit., Article 3

intruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun (Pasal 30).

Harga sebuah program komputer/*software* yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis untuk menggandakan serta menjual *licensi software* bajakan dengan harga yang sangat murah. Misalnya, program anti virus seharga $ 75 dapat dibeli dengan harga Rp 50.000,00. Harga penjualan yang sangat murah dibandingkan dengan software asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 perkeping.

Maraknya pembajakan software di Indonesia yang terkesan "dimaklumi" hal ini sangat merugikan pemilik hak cipta. Tindakan pembajakan *software* tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu :[101]

> "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah)"

5. Undang-undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang-undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang.

Undang-undang ini merupakan yang paling tepat bagi penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang

[101] Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta

termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-undang Perbankan.

Dalam Undang- Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan. Dalam Undang- Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat diperoleh dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data-data tersebut. Undang-undang ini juga mengatur mengenai alat bukti elektronik (*digital evidence*) sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

6. Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Selain Undang-undang Nomor 25 Tahun 2003 Undang-undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. Digital evidence atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah e-mail dan chat room selain mencari informasi dengan menggunakan search engine serta melakukan propaganda melalui *bulletin board atau mailing list*.

7. Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik

Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik ini dibuat dalam rangka melihat globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengeolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan

secara optimal, merata dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa. Maka disamping Undang-undang Nomor 36 Tahun 1999, Indonesia memerlukan Undang-undang Internet (*Law of Internet*) atau Undang-undang *cyber* (*Cyber Law*). Undang- Undang Internet sebagai suatu aturan hukum yang baru akan lebih memudahkan untuk dipahami dengan mengetahui ruang lingkup pengaturannya. Undang-undang Internet merupakan undang-undang khusus mengatur secara eksplisit hal-hal yang menyangkut pengiriman dan penerimaan informasi secara elektronik melalui Internet. Bila Undang-undang ini dihubungkan dengan Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi, maka Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi akan merupakan *lex generalis* sedangkan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik merupakan *lex specialis* dari Undang-undang Telekomunikasi tersebut. Dilihat dari sisi perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru mendukung tekhnologi informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia.[102]

[102] Raida L. Tobing, *Jurnal Akhir Penelitian Hukum Tentang Efektifitas Undang-undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik*, Jakarta, Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI,2010 halaman.48 .

keberadaan Undang-undang ini adalah memberikan kepastian hukum terhadap keberadaan suatu data atau informasi yang dihasilkan oleh sistem elektronik berikut akunbilitas sistem elektronik itu sendiri dilengkapi dengan beberapa ketentuan hukum yang mengatur penyelenggaraannya dan akibat pemanfaatannya tersebut baik untuk kepentingan hukum individual, komunal maupun nasional bahkan international.[103]

Dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik diatur beberapa aspek, diantaranya adalah sebagai berikut:[104]

a. Aspek yuridis, digunakan pendekatan prinsip perluasan Yurisdiksi *(Extra Territorial Yurisdiction)* dikarenakan transaksi elektronik memiliki karakteristik lintas teritorial dan tidak dapat menggunakan pendekatan hukum konvesional;
b. Aspek pembuktian elektronik (*e-evindence*), alas bukti elektronik merupakan alat bukti dan memiliki akibat hukum yang sah di muka pengadilan;
c. Aspek informasi dan perlindungan konsumen, pelaku usaha yang menawarkan produk melalui media elektronik wajib menyediakan informasi yang lengkap dan benar, berkaitan dengan syarat – syarat kontrak, produsen dan produk yang ditawarkan;

[103] Ahmad M, Ramli, *Jurnal Tim Perencanaan Pembangunan Hukum Nasional Bidang Teknologi Informasi dan Komunikasi*, Jakarta, Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI,2008 , halaman.53.

[104] *Ibid.,* hlm 48.

d. Aspek tanda tangan elektronik, memiliki kekuatan hukum dan akibat hukum yang sah (sejajar dengan tanda tangan manual) selama memenuhi persyaratan sebagaimana ditetapkan di dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik;
e. Aspek pengamanan terhadap tanda tangan elektronik, setiap orang yang terlibat dalam tanda tangan elektronik berkewajiban memberikan pengamanan atas tanda tangan elektronik yang digunakannya;
f. Aspek penyelenggara sertifikasi elektronik, setiap orang berhak menggunakan jasa penyelenggara sertifikasi elektronik untuk tanda tangan elektronik yang dibuat
g. Aspek penyelenggaraan sertifikasi elektronik, informasi dan transaksi elektronik diselenggarakan oleh penyelenggara sistem elektronik secara andal, aman, dan beroperasi sebagaimana mestinya serta penyelenggara sistem elektronik bertanggung jawab terhadap penyelengaraan/kemanan sistem elektronik yang diselenggarakannya;
h. Aspek tanda tangan digital (*Digital Signature*), penggunaan digital signature dapat berubah sesuai dengan isi dokumen dan memiliki sifat seperti tanda tangan konvesional sepanjang dapat dijamin keadalannya secara teknis;
i. Aspek transaksi elektronik, kegiatan transaksi elektronik dapat dilakukan baik dalam lingkup publik maupun privat dan transaksi elektronik yang dituangkan dalam kontrak elektronik mengikat para pihak, serta para pihak

memiliki kewenangan untuk memilih hukum yang berlaku bagi transaksi elektronik internasional yang dibuatnya;

j. Aspek nama domain (*domain names)*, yang digunakan sebagai Hak Kekayaan Intelektual (HaKI) oleh seseorang, orang dimaksud berhak memiliki nama domain berdasarkan prinsip *first come first serve* dan informasi elektronik yang disusun menjadi karya intelektual y.n, ada di dalamnya, dilindungi sebagai HaKI berdasarkan perUndang-undangan yang berlaku;

k. Aspek perlindungan *privacy*, penggunaan setiap informasi melalui media elektronik yang menyangkut data tentang pribadi seseorang harus dilakukan atas persetujuan bagi orang yang bersangkutan, kecuali ditentukan lain oleh per Undang-undangan;

l. Aspek peran Pemerintah dan masyarakat, Pemerintah memfasilitasi pemanfaatan informasi dan transaksi elektronik dengan memperhatikan ketentuan peraturan perundang-undangan yang berlaku;

m. Aspek perlindungan kepentingan umum, Pemerintah berwenang melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi dan transaksi elektronik yang mengganggu ketertiban umum dan kepentingan nasional serta Pemerintah menetapkan instansi tertentu harus memiliki back-up e-data dan data on-line ; dan

n. Aspek perbuatan – perbuatan yang dilarang adalah:

   1. Menyebarkan informasi elektronik yang bermuatan pornografi, perjudian, tindak kekerasan, penipuan;

2. Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik;
3. Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik milik Pemerintah yang karena statusnya harus dirahasiakan atau dilindungi;
4. Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik menyangkut pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap Negara dan atau hubungan dengan subjek hukum internasional;
5. Melakukan tindakan yang secara tanpa hak yang transmisi dari program, informasi, kode atau perintah, komputer dan atau sistem elektronik yang dilindungi Negara menjadi rusak; dan
6. Menggunakan dan mengakses komputer dan atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer dan atau sistem elektronik yang dilindungi oleh Negara.

Sedangkan asas – asas yang berlaku di Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik berdasarkan pada Pasal 3, maka pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik dan kebebasan memilih teknologi atau netral teknologi. Kehadiran Undang-undang ini diharapkan akan memberikan manfaat, beberapa diantara nya :

1) Menjamin kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik;
2) Mendorong pertumbuhan ekonomi indonesia;
3) Sebagai salah satu upaya untuk mencegah terjadinya kejahatan berbasis teknologi informasi;
4) Melindungi masyarakat pengguna jasa dengan memanfaatkan teknologi informasi;

Dalam ini secara rinci dijelaskan mengenai perbuatan-perbuatan yang dilarang atau segala perbuatan yang digolongkan tindak pidana kejahatan komputer diatur di Bab VII dalam Pasal 27 sampai dengan Pasal 37. Sedangkan di BAB IX yang terdiri atas Pasal 45 sampai dengan Pasal 52 menentukan kriminalisasi tehadap perbuatan - perbuatan yang dilarang atau segala perbuatan yang digolongkan tindak pidana komputer.

Materi muatan dari Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik adalah menyangkut masalah yurisdiksi, perlindungan hak

pribadi, asas perdagangan secara *e-commerce*, asas persaingan usaha tidak sehat dan perlindungan konsumen, asas hak atas kekayaan intelektual (HAKI) dan hukum Internasional serta asas *cybercrime*. Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik mengkaji *cyber case* dalam beberapa sudut pandang secara komprehensif dan spesifik, fokusya adalah semua kegiatan yang dilakukan dalam dunia maya, kemudian ditentukan pendekatan mana yang paling cocok untuk regulasi *Cyber law* di Indonesia.

E. Ruang Lingkup *Cybercrime*

Dalam melihat ruang lingkup *cybercrime* harus didasarkan pada undang-undang yang mengaturnya. Undang-undang yang dimaksud adalah Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik.

Dalam undang-undang tersebut pada Pasal 1 ayat (2) disebutkan bahwa:

Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.[105] Merujuk dari pasal tersebut, dapat dipahami bahwa transaksi elektronik sebagai suatu perbuatan hukum yang dilakukan dengan komputer dan jaringan komputer, dapat juga dilakukan melalui sarana/media elaktronik lainnya, seperti *laptop, Notebook* dan *smartphone*.

[105]Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik.

Berkaitan dengan hal tersebut, untuk mengetahui lebih lanjut tentang ruang lingkup *cybercrime* dapat juga dilihat melalui pengertian *cybercrime* sebagai berikut:

Pada pembahasan sebelumnya disebutkan bahwa, *Cybercrime* adalah kejahatan yang muncul sebagai dampak negatif dari perkembangan aplikasi internet.[106] Pengertian ini membatasi pada ruang aplikasi internet, sehingga jika pelaku menggunakan LAN (*local area network*), maka akan lepas dari target hukum. Karena hanya dibatasi oleh sarana internet meskipun sama-sama menggunakan media komputer. Oleh karena itu, definisi tersebut tidak menyebutkan media elektronik tertentu, tetapi memfokuskan pada dampak aplikasi internet.

Sedangkan menurut Kepolisian Inggris, *cybercrime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.[107]

Pengertian tersebut menarik, karena pengertian ini memiliki kesamaan dengan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik, yakni menggunakan jaringan komputer. Dari 2 (dua) pengertian tersebut yang menjadi catatan adalah bahwa dalam definisi tersebut tidak dijelaskan apa maksud kata "jaringan komputer". Apabila dimaknai secara luas maka akan meliputi LAN (*local area networking*) dan internet. LAN ini mempunyai karakter yang berbeda

---

[106] http://www.thecelia.com/dokumen/jurnal/ajo.a002.shtml. Diakses pada tanggal 25 Juli 2019)

[107] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* Cet. I, Bandung, Refika Aditama, 2005, Halaman 40.

dengan internet. LAN merupakan jaringan tertutup. Dalam beberapa segi, jenis kejahatan yang disebut termasuk dalam katagori *cybercrime* tidak dapat dilakukan dalam LAN ini, seperti *spamming, cybersquatting*.

Dengan demikian media elektronik apapun yang dapat digunakan sebagai sarana teraksesnya internet dan transaksi elektronik merupakan bagian yang dimaksudkan oleh Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi elektronik. Sehingga, siapapun sebagaimana dimaksud dalam undang-undang yang melakukan kejahatan dalam ruang dan batas sebagaimana dijelaskan, maka di kategorikan sebagai tindak kejahatan dunia maya (*cybercrime*). Oleh karena itu, menjadi terbedakan antara tindak pidana *cybercrime* dan konvensional. Dalam *cybercrime* tidak terjadi kontak fisik antara subyek dan obyek melainkan melalui media elektronik. Sedangkan kejahatan konvensinal melalui kontak fisik secara langsung yang dengan mudah diketahui pelakunya atau subyek nya.

BAB III

AKSES SISTEM KOMPUTER SECARA ILEGAL (*HACKING)* DAN MENIMBULKAN KERUSAKAN (*CRACKING)* DALAM HUKUM PIDANA DI INDONESIA

A. Defenisi *Hacking* dan *Cracking*

Peraturan perundang-undangan di Indonesia tidak mengenal istilah *hacking*. Secara harafiah *"hacking"* berasal dari kata *"hack"* dari bahasa Inggris yang berarti mencincang atau membacok. Namun dalam kejahatan internet *hacking* dapat diartikan sebagai penyusupan atau perusakan suatu sistem komputer.[108] *Hacking* merupakan aktivitas penyusupan/akses ilegal ke dalam sebuah sistem komputer ataupun jaringan dengan tujuan untuk menyalahgunakan ataupun merusak sistem yang ada. Definisi dari kata "menyalahgunakan" memiliki arti yang sangat luas, dan dapat diartikan sebagai pencurian data rahasia, serta penggunaan *email* yang tidak semestinya seperti *spamming* ataupun mencari celah jaringan yang memungkinkan untuk dimasuki.

Banyak orang menganggap bahwasanya istilah *hacking* dan *cracking*, merupakan sebuah hal yang sama, oleh sebab itu perlu ditekankan bahwa ada perbedaan mendasar antara *hacking* dan *cracking* ini. Kesalahan dalam penyebutan istilah ini menyebabkan konstruksi makna yang berkembang di masyarakat menjadi tidak benar dan konstruksi ini tampaknya sampai sekarang tetap ada dan terpelihara, terbukti dengan pemberitaan media yang masih menempatkan *Hacker* sebagai pelaku *Cybercrime*. Perbedaan yang mendasar

[108] Sudarto, *Kapita Selekta Hukum Pidana*, Bandung, Alumni, 1981, halaman. 38

antara *hacking* dan *cracking* ini adalah terletak pada efek perbuatannya. Secara umum *hacking* adalah kegiatan melakukan akses kedalam suatu sistem dengan cara yang tidak sah atau ilegal, selanjutnya jika tindakan yang dilakukan menimbulkan kerusakan atau bersifat *destruktif* maka disebut sebagai *cracking*. Orang yang melakukan hacking disebut disebut sebagai hacker sedangkan yang melakukan *cracking* disebut *cracker*. Namun terlepas dari kedua hal tersebut, keduanya tetap melakukan suatu akses yang ilegal. Sebagaimana akan diuraikan perbedaan antara *hacking* dan *cracking* dalam tabel berikut:

Keterangan	***Hacking***	***Cracking***
Jenis Kegiatan	Akses Ilegal (Masuk kedalam sistem komputer orang lain tanpa hak/ tidak sah)	Akses Ilegal (Masuk kedalam sistem komputer orang lain tanpa hak/ tidak sah) dan melakukan perusakan
Dampak yang ditimbulkan	Tidak ada kerusakan sistem, malahan ada unsur membangun (memberitahu administrator bahwa sistem keamanan rentan penyusupan), namun sedikit atau banyak akan mempengaruhi dari sitem komputer/atau suatu	Sistem menjadi rusak dan bahkan bisa menjadi mati total dan tidak berfungsi/*Down*

Keterangan	*Hacking*	*Cracking*
	jaringan informasi	
Etika	Mempunyai Etika dalam melakukan *hacking*	Tidak mempunyai etika , dilakukan hanya sekedar iseng dan menunjukan eksistensi dirinya

Kongres PBB X di Wina, menetapkan *Hacking* dan *cracking* sebagai *first crime*. Ini disebabkan karena kejahatan tersebut merupakan suatu yang istimewa karena mempunyai kelebihan tertentu dibanding kejahatan *cyber* yang lain. Kelebihan dari kejahatan ini antara lain yaitu, pertama, orang yang dapat melakukan kejahatan jenis ini sudah barang tentu dapat melakukan kejahatan *cybercrime* yang lain. Kedua, secara teknis imbas dari aktivitas *hacking* kualitas yang dihasilkan lebih serius dibandingkan dengan bentuk *cyber crime* yang lain. Untuk menyebarkan gambar porno atau *cyber phornography* tidak perlu memiliki kemampuan *hacking*, cukup kemampuan minimal tentang internet.

Hacker di bagi dua kategori: *White-Hat Hackers* (Hacker topi putih), yaitu tokoh-tokoh yang mengagumkan dari segi pencapaian teknis dan filosofis mereka yang turut mengembangkan budaya *hacker* di dunia. Ini adalah tokoh-tokoh yang ikut mendorong banyak revolusi dalam dunia komputer dan teknologi informasi. Mereka yang berani melakukan kreatifitas di luar kebiasaan sehari-hari. Merekalah pemikir-pemikir *out-of-the-box*, revolusionis dalam dunia yang semakin kabur. Tokoh-tokoh tersebut antara lain : Tim Berners-Lee (Sang

Penemu Web), Linus Torvalds (Pemikir *Linux*), Richard Stallman (Penggagas GNU) dan Gordon Lyon (Pembuat Nmap).

kelompok kedu yaitu *Black-Hat Hackers* (Hacker topi hitam) merupakan cikal bakal dari *cracker*, adalah tokoh-tokoh yang kerap melupakan batasan moral dan etika dalam melakukan inovasi teknologi. Mereka juga ikut mendorong banyak revolusi dalam dunia komputer dan teknologi informasi, salah satunya dari sisi pihak- pihak yang tak ingin lagi menjadi korban dari aksi-aksi para *Black-Hat ini*. Tokoh-tokoh Black-Hat adalah: Robert Tappan Morris {Pembuat Worm (*Worm- Virus*) Pertama Di Dunia}, Kevin Mitnick (*America's Most Wanted Hacker*), Vladimir Levin (Pembobol Citibank Agustus 2004), Loyd Blankenship (*The Mentor*), Kevin Poulsen ("*Win a Porsche by Friday". Lotere by U.S radio*), Joe Engresia (*Phreaker* Buta yang Legenda), John Draper (*Captain Crunch, Crunchman,* atau *Crunch*), serta Adrian Lamo (Pembobol Yahoo!, Microsoft, Excite@Home, World Com, New York Times).

Dalam sejarah *Hacker*, apa yang dilakukan oleh para *Hacker* itu selalu ada kaitannya dengan pengembangan sistem keamanan komputer. Keamanan komputer itu penting untuk melindungi data-data atau informasi yang bersifat rahasia dan agar tetap terjaga kerahasiaannya maka sistem keamanan yang ada dan digunakan untuk melindunginya perlu secara terus-menerus dimodifikasi atau selalu dijaga kemutakhirannya. Tugas *Hacker* adalah menguji sistem keamanan ini dan memperbaiki sistem atau program keamanannya sehingga tidaklah

mengherankan jika seorang *Hacker* adalah programer (tetapi tidak setiap programer bisa menjadi *Hacker*).[109]

Secara lebih spesifik *hacker* didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengaman lainnya, tetapi tidak melakukan tindakan pengrusakan apapun, tidak mencuri uang atau informasi.Sedangkan *cracker* adalah sisi gelap dari *hacker* dan memiliki ketertarikan untuk mencuri infomasi, melakukan berbagai macam pengrusakan dan sesekali waktu juga melumpuhkan keseluruhan sistem komputer. Perbedaan terminologi antara *hacker* dan *cracker* terkadang menjadi bias dan hilang sama sekali dalam perspektif media masa dan masyarakat umum. Para *cracker* juga tidak jarang menyebut diri mereka sebagai *hacker* sehingga menyebabkan citra *hacking* menjadi buruk.[110] Mereka inilah yang disebut dengan *Hacker* topi Hitam (*Black-Hat*).

Dalam *The New Hacker's Dictionari* disebutkan bahwa yang dimaksud dengan *Cracker* adalah :

> *One who breaks security on a system. Coined by hackers in defense against journalistic mususe of the term "hacker". The term "cracker" reflects a strong revulsion at the theft and vandalism perpetrated by cracking rings. There is far less overlap between hackerdom and crakerdom than most would suspect.*[111]

---

[109] Selain berkaitan dengan pengembangan sistem keamanan kompter atau jaringan komputer, seorang Hacker yang melakukan Hacking juga sangat bermanfaat dalam meningkatkan kecepatan program dan menghemat sumber daya yang ada. Kelemahan yang dimiliki oleh sebuah program akan diketahui oleh seorang Hacker dan ia akan memberitahukan kepada pemilik atau pembuat program untuk segera memperbaiki atau menyempurnakan. Dari kelemahan sebuah program yang telah diketahui, tidak hanya program itu yang dapat disempurnakan, tetapi kecepatan yang dimiliki sebuah komputer

[110] Richard Mansfield, *Hacker Attack*, Manhattan, Sybex, 2000, halaman. 23

[111] Eric S. Raymond. *The New Hacker's Dictionary*, MIT Press, versi elektronik dapat dilihat pada http://webyes.com.br/wp-content/uploads/ebooks/book_the_hacker_dictionary.pdf , Akses tanggal 28 Juli 2019

Salah satu yang membedakan antara *Hacke*r (atau yang oleh Paul Taylor disebut sebagai *Computer Security Industry*) dan *Cracker* (*Computer Underground*) adalah masalah etika. Ada beberapa tokoh *Hacker* yang mengedepankan bahwa etika lah yang membedakan antara *Hacker* dan *Cracker* di antaranya adalah *Loyd Blankenship* alias *The Mentor* yang tergabung dalam *Legion of Doom/Legion of Hackers*. Etika *Hacker* yang dimaksud oleh *The Mentor* adalah sebagai berikut :[112]

a. *Do not intentionally damage "any" system.*
b. *Do not alter any system files othe than ones needed to ensure your escape fram detection and your future access (Trojan Horses, Altering Logs and the like are all necessary to your survival for as long as possible).*
c. *Do not leave your (or anyone else's) real name, real handle or real phone number on any system that you access illegally. They "can" and will track you down from your handle!*
d. *Be careful who you share information with. Feds are getting trickier. Generally, if you don't know their voice phone number, name and occupation or haven't spoken with them voice on non-info trading conversations, be wary.*
e. *Do not leave your real phone number to anyone you don't know. This includes logging on boards, no matter how k-rad they seem. If you don't know the sysop, leave a note telling some trustworthy people that will validate you.*
f. *Do not hack government computers. Yes, there are government systems that are safe to hack, but bhey are few and far between. And the government has inifitely more time and resources to track you down than a company who has to make a profit and justify expenses.*
g. *Do not use codes unless there is "NO" way around it (you don't have a local telenet or tymnet outdial and can't connect to anything 800…) you use codes long enough, you will get caught. Period.*
h. *Do not be afraid to be paranoid. Remember, you "are" breaking the law. It doesn't hurt to store everything encrypted on your hard disk or keep your notes buried in the backyard or in the trunk of your car. You may feel a little funny but you'll feel a lot funnier when you when you meet Bruno, your transvestite cellmate who axed his family to death.*
i. *Watch what you post on boards. Most of the really great hackers in the country post "nothing" about the system they're currently working except*

[112] The Mentor, *A Novice's Guide to Hacking*, edisi 1989, versi elektronik dapat dilihat pada https://www.netsaber.com.br/apostilas/apostilas/1718.pdf, akses tanggal 28 juli 2019

in the broadest sense (I'm working on a UNIX, or a COSMOS, or something generic. Not "I'm hacking into General Electric's Voice Mail System" or something inane and revealing like that).

j. Do not be afraid to ask questions. That's what more experienced hackers are for. Don't expect "everything" you ask to be answered, though. There are some things (LMOS, for instance) that a beginning hacker shouldn't mess with. You'll either get caught or scres it up for others or both.

k. Finally, you have to actually hack. You can hang out on boards all you want, and you can read all the text files in the word but until you actually start doing it, you'll never know what it's all about. There's no thrill quite the same as getting into your first system (well, ok, I can think of a couple of bigger thrills, but you get the picture).

Cracker tidak punya niat atau kemauan untuk mengikuti etika itu. Ketidakmauan atau tidak adanya niat *Cracker* untuk mematuhi etika *Hacker* terbukti dengan aksi mereka yang telah merusak sistem komputer suatu perusahaan atau lawan politiknya, menyerang dan merusak situs-situs pemerintah atau pelayanan publik dan situs-situs yang memberikan layanan pendidikan dan penelitian.

B. Tahapan-tahapan dalam Melakukan *Hacking* dan *Cracking*

Dalam melakukan aksinya, tahapan-tahapan yang dilakukan oleh *hacker* dan *cracker* kurang lebih sama, sedangkan yang membedakan adalah efek yang ditimbulkan. Keberhasilan dalam melakukan *hacking* terjadi apabila seorang *hacker* dapat mengakses kedalam suatu sistem yang dituju. Sedangkan apabila sistem yang dimasuki kemudian dirusak dan mengalami kerusakan maka disebut *cracking.* Adapun modus operandi yang dilakukan oleh para *hacker* dan *cracker* dalam pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik biasanya disebut *Unauthorized Acces to Computer System and Service*

yaitu kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik resmi sistem jaringan komputer yang dimasukinya. Secara umum tahapan-tahapan dalam dalam proses *hacking* dan *cracking* adalah sebagai berikut:

1) *Footprinting*

Footprinting dan/atau pencarian data *cracker* baru mencari sistem yang dapat disusupi. *Footprinting* merupakan kegiatan mencari data berupa: menentukan ruang lingkup atau *scope* aktivitas atau serangan, *network enumeratin* atau menyeleksi jaringan, introgasi jaringan, mengintai jaringan. Semua kegiatan ini dapat dilakukan dengan alat atau *tools* dan merupakan informasi yang tersedia bebas di *internet*. Kegiatan *footprinting* ini dapat diibaratkan mencari informasi yang tersedia umum melalui buku telepon.[113]

2) *Scanning*

Scanning atau pemilihan sasaran lebih bersifat aktif terhadap sistem sasaran. Disini diibaratkan *cracker* sudah mulai mengetuk-ngetuk dinding sistem sasaran untuk mencari apakah ada kelemahannya. Kegiatan *scanning* dengan demikian dari segi jaringan sangat berisik dan mudah dikenali oleh sistem yang dijadikan sasaran, kecuali dengan menggunakan *stealth scanning*. *Scanning tool* yang paling legendaris adalah *nmap* (yang kini tersedia pula untuk *Windows 9x/ME* maupun DOS), selain *superscan* dan *ultrascan* yang juga digunakan pada sistem *windows*. Untuk melindungi diri dari kegiatan *scanning* adalah memasang

[113] Nur Khalimatus Sa'diyah, "*Perspektif, Modus Operandi Tindak Pidana Cracker Menurut Undang-undang Informasi dan Transaksi Elektronik",* Volume XVII Nomor 2, Mei 2012), halaman 83.

firewall misalnya *zone alarm*, atau bila ada keseluruhan *network*. Dengan menggunakan aplikasi *intrusion detection system* (IDS) misalnya *snort*.[114]

3) Enumerasi

Enumerasi atau pencarian data mengenai sasaran sudah bersifat sangat *intrusif* (mengganggu) terhadap suatu sistem. Disini para penyusup dapat mencari *account name* yang absah, *password*, serta *share resources* yang ada. Pada tahap ini, khusus untuk sistem *windows*, terdapat port 139 (*NetBIOS session service*) yang terbuka untuk *resourch sharing* antar pemakai dalam jaringan. Beberapa orang mungkin berpikir bahwa *harddisk* yang di *share* itu hanya dapat dilihat oleh pemakai dalam *LAN* saja. Kenyataannya tidak demikian, *netBIOS session service* dapat dilihat oleh siapapun yang terhubung ke *internet* di seluruh dunia. *Tool* seperti *legion, SMB Scanner*, atau *shares* folder membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka *resource share* tanpa pemberian *password*).[115]

4) Gainning acces

Gainning acces atau dikatakan akses ilegal telah ditetapkan adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai *user* biasa. Ini adalah kelanjutan dari kegiatan *enumerasi* , sehingga biasanya disini seorang penyerang sudah mempunyai paling tidak *user account* yang absah, dan tinggal mencari *passwordnya* saja. Bila *resource share-nya* diproteksi dengan suatu *password*, maka *password* ini dapat saja ditebak (karena banyak yang

[114] *Ibid.,*
[115] *Ibid.,*

menggunakan *password* sederhana dalam melindungi komputernya). Menebaknya dapat secara otomatis melalui *dictionary attack* (mecoba kata-kata dari kamus sebagai suatu *password*) atau *brute-force attack* (mencobakan kombinasi semua karakter sebagai *password*). Dari sini penyerang mungkin akan berhasil memperoleh *log-on* sebagai *user* yang absah.[116]

5) Escalating privelege

Escalating privelege (menaikkan atau mengamankan suatu posisi) mengasumsikan bahwa penyerang sudah mendapat *log-on acces* pada sistem sebagai *user* biasa. Penyerang kini berusaha naik kelas menjadi *admin* (pada sistem windows) atau menjadi *root* (pada *sistem unix atau linux*). Teknik yang digunakan sudah tidak lagi *dictionary attack* atau *brute-force attack* yang memakan waktu itu, melainkan mencuri *password* file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem *windows 9x/ME password* disimpan dalam *file PWL* sedangkan *windows NT/2000* dalam *file SAM*. Bahaya pada tahap ini bukan hanya dari penyerang diluar sistem melainkan lebih besar lagi bahayanya adalah orang dalam, yaitu *user* absah dalam jaringan itu sendiri yang berusaha naik kelas menjadi *admin* atau *root*.[117]

6) Pilfering

Pilfering atau suatu proses pencurian, proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke

---

[116] *Ibid*.,
[117] *Ibid.,*Halaman 84

trusted system. Mencakup evaluasi *trust* dan pencarian *cleartext password* di *registry*, *config file*, dan *user* data.[118]

7) Covering tracks

Convering tracks atau menutup jejak, begitu kontrol penuh terhadap sistem yang diperoleh, maka menutup jejak menjadi suatu prioritas. Meliputi membersihkan *network log* dan penggunaan *hide tool* seperti macam-macam *rootkit* dan *file streaming*.[119]

8) Creating backdoors

Creatif blackdoors atau membuat jalan pintas, pintu belakang diciptakan pada berbagai bagian dari suatu sistem untuk memudahkan masuk kembali. Pada tahap keenam, ketujuh, dan kedelapan, penyerang sudah berada dan menguasai suatu sistem dan kini berusaha untuk mencari informasi lanjutan atau *pilfering,* menutupi jejak penyusupannya atau *convering tracks*, dan menyiapkan pintu belakang atau *creating backdoor* agar lain kali dapat dengan mudah masuk lagi ke dalam sistem. Adanya *trojan* pada suatu sistem berarti suatu sistem dapat dengan mudah dimasuki penyerang tanpa harus berusaha payah melalui tahapan-tahapan diatas, hanya karena kecerobohan pemakai komputer itu sendiri.[120]

9) Denial of service

Denial of service atau melumpuhkan sistem, bukan tahapan terakhir, melainkan kalau penyerang sudah frustasi tidak dapat masuk ke dalam sistem

---

[118] *Ibid.,*
[119] *Ibid.,*
[120] *Ibid.,*

yang kuat pertahanannya, maka dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu *crash* atau kacau. *Denial of service attack* sangat sulit dicegah, sebab memakan habis *bandwidth* yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para *script kiddes* yang pengetahuan *crackingnya* terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.[121]

Langkah *Hacker* dan *cracker* setelah mengetahui sistem operasi apa yang dipakai pada target sasaran adalah menyusup atau mengakses jaringan komputer target sasaran itu. Dengan kata lain, *Hacker* dan *cracker* memasuki situs orang lain tanpa izin. Hacker dengan kemampuannya dapat masuk dan berjalan-jalan dalam situs orang lain meskipun situs itu telah dilengkapi dengan sistem keamanan. Jika akan membuka sebuah Website, misalnya website Bank Mandiri dengan alamat ”www.mandiri.co.id” nya, maka akan muncul tampilan yang dapat dibaca ataupun di download. Apa yang ditampilkan dalam situs Bank Mandiri tersebut dapatlah disebut sebagai ruang yang bisa dilihat dan dinikmati oleh pengunjung situs itu. Itulah yang dinamakan ruang publik atau ruang untuk pelayanan publik atau disebut juga ruang yang bersifat terbuka.

Apabila di gambarkan bahwa sebuah Website adalah seperti sebuah rumah dengan pekarangannya, maka apa yang bisa dilihat dari luar, itulah yang bisa diberikan oleh pemilik rumah untuk dinikmati oleh orang lain sebagai perwujudan dari fungsi sosial rumah itu. Akan tetapi, apabila orang ingin masuk ke rumah itu

---

[121] *Ibid*

(meskipun hanya ingin masuk tanpa maksud lain apapun), maka ia harus mendapat izin dari pemilik rumah, jika tetap nekad untuk masuk, maka ia dapat didakwa melanggar privasi orang apalagi jika diikuti dengan tindakan lain yang bersifat merugikan. Memasuki ruang privat dalam sebuah situs internet jelas-jelas dilarang karena akan menyebabkan terganggunya fungsi ruang privat itu apalagi jika diikuti dengan tindakan lanjut yang bersifat destruktif. Mengingat hal tersebut, mala langkah kedua dari Hacking ini sudah dapat dikategorikan sebagai kejahatan. Apabila dimasuki dan informasi yang ada di dalamnya disebar-luaskan, maka hal tersebut akan menimbulkan kerugian yang tidak sedikit jumlahnya.

C. Faktor – Faktor yang Mempengaruhi Terjadinya *Hacking* dan *Cracking*

Di era kemajuan teknologi informasi ditandai dengan meningkatnya pengguna internet dalam setiap aspek kehidupan manusia. Meningkatnya pengguna internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan suatu aktivitasnya. Disisi lain memudahkan bagi pihak-pihak tertentu untuk dapat melakukan tindak pidana.[122] Munculnya kejahatan dengan mempergunakan internet sebagai alat bantunya. Lebih banyak disebabkan oleh faktor keamanan si pelaku dalam melakukan kejahatan. Dan masih kurangnya aparat penegak hukum yang memiliki kemampuan dalam penguasaan informasi dan teknologi. Berikut ini merupakan

[122] Didik M. Arief Mansur dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi*, Bandung, Refika Aditama, 2006, halaman 95.

faktor-faktor yang mempengaruhi terjadinya *hacking* dan *cracking*, antara lain adalah:

1. Faktor politik

Dengan mencermati masalah *hacking* dan *cracking* yang terjadi di Indonesia dengan permasalahan yang dihadapi oleh aparat penegak hukum, proses kriminalitas dibidang *hacking* dan *cracking* telah terjadi dan merugikan masyarakat. Yang dilakukan oleh orang Indonesia, sebagaimana kasus yang telah terjadi dibeberapa kota di Indonesia mengakibatkan citra Indonesia kurang baik di mata dunia dalam pengakuan hukum *hacking* dan *cracking*.[123]

Serangan serangan para *hacker* maupun *cracker* dapat merusak jaringan komputer yang digunakan oleh pemerintah, perbankan, pelaku usaha maupun perorangan yang berdampak terhadap kekacauan dalam sistem jaringan. Dapat dipastikan apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari saja maka dapat menimbulkan kekacauan pembayaran maupunn transaksi keuangan bagi nasabah. Kondisi ini memerlukan kebijakan politik pemerintah indonesia untuk menanggulangi cracker yang berkembang di Indonesia. Untuk menghindari kerugian yang lebih besar akibat tindakan para cracker maka diperlukan suatu kebijakan politik pemerintah Indonesia untuk menyiapkan perangkat hukum khusus *(lex spesialis)* bagi *hacker* dan *cracker* yang saat ini telah diwujudkan dengan adanya Undang-undang ITE.

---

[123] Nur Khalimatus Sa'diyah, "*Perspektif, Modus Operandi Tindak Pidana Cracker Menurut Undang-undang Informasi dan Transaksi Elektronik*" (Volum XVII No.2, Mei 2012), halaman 83

2. Faktor ekonomi

Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi. Jaringan komputer dan internet merupakan media yang sangat murah untuk promosi. Masyarakat dunia banyak yang memanfaatkan ini untuk mencari barang-barang kepentingan perorangan meupun korporasi. Adapun krisis ekonomi yang telah melanda bangsa Indonesia harus dijadikan pelajaran bagi masyarakat Indonesia untuk segera bangkit dari krisis tersebut. Seluruh komponen bangsa Indonesia harus berpartisipasi mendukung pemulihan ekonomi. Media internet dan jaringan komputer merupakan salah satu media yang dapat dimanfaatkan oleh seluruh masyarakat untuk mempromosikan Indonesia.

3. Faktor sosial budaya

Faktor sosial budaya dapat dilihat dari beberapa aspek, yaitu:[124]

a) Kemajuan teknologi informasi

Pesatnya kemajuan teknologi informasi sungguh tidak dapat deibendung oleh siapapun dinegara ini. Semua orang membutuhkan teknologi, informasi bahkan levelitas kebutuhan itu terhadap orang-orang tertentu yang maniak informasi dianggapnya sebagai sebuah kebutuhan primer. Dengan adanya teknologi informasi manusia dapat melakukan akses perkembangan lingkungan secara akurat, karena disitu ada kebebasan yang seimbang, bahkan dapat saja mengaktualisasikan dirinya agar dapat dikenali oleh lingkungannya. Menurut Agus Raharjo setidaknya ada dua hal yang membuat teknologi informasi dianggap suatu celah atau

[124] *Ibid.,*

bug dalam memacu ekonomi dunia : teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya; dapat memudahkan transaksi bisnis terutama bisnis keuangan disamping bisnis-bisnis umum lainnya.[125]

b) Sumber daya manusia (SDM)

Yang mengawali antara teknologi informasi dengan operator yang mengawaki mempunyai hubungan yang sangat erat sekali, keduanya tak dapat dipisahkan. Sumber daya manusia dan teknologi informasi mempunyai peranan yang sangat penting sebagai pengendali dari sebuah alat. Di Indonesia sumber daya pengelolaan teknologi informasi ini cukup, namun sumber daya manusia untuk memproduksi atau menciptakan suatu teknologi masih kurang. Penyebabnya ada berbagai hal, diantaranya kurang adanya tenaga peneliti dan kurangnya biaya penelitian atau kurangnya perhatian dan apresiasi terhadap penelitian. Sehingga sumber daya manusia di Indonesia lebih banyak sebagai penguna saja dan jumblahnya cukup banyak.

c) Komunitas baru

Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, diantaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologis terbentuklah sebuah komunitas baru di dunia maya yakni komunitas para pecandu internet yang saling berkomunikasi dan bertukar

---

[125] Agus Raharjo, *Cyber crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung, Citra Aditya Bakti, 2002, halaman 1.

pikiran berdasarkan prinsip kebebasan dan keseimbangan diantara para pecandu dunia maya tersebut.[126]

d) Dampak *hacking* dan *cracking* terhadap keamanan Negara

Setelah melihat dari beberapa faktor yang mepengaruhi terjadinya *hacking* dan *cracking* terhadap keamanan negara yaitu dapat disoroti dari beberapa aspek, antara lain: kurangnya kepercayaan dunia terhadap Indonesia, di sejumlah kota-kota besar yang ada seperti Bandung, Semarang, Yogyakarta Surabaya dan Jakarta, para *hacker* dan *cracker* sebagian besar itu adalah dari oknum terdidik seperti mahasiswa. Hukuman terhadap *cracker* dulunya cukup ringan, bahkan banyak pihak berpendapat, pelakunya adalah pahlawan karena dapat membobol suatu situs dengan kemmapuannya. Padahal, dibalik kejahatan itu para pelaku telah menurunkan derajat dan martabat bangsa Indonesia di mata dunia, karena banyak merugikan banyak pihak melalui teknologi informasi.[127]

e) Dapat berpotensi menghancurkan negara

Perkembangan dari teknologi informasi yang ada membawa suatu dampak lain, yaitu tumbuh suburnya *hacker* dan *cracker*, kejahatan melalui media internet, *hacker* dan *cracker* menjadi masalah serius yang harus segera ditangani. Kepolisian dan para penegak hukum lainnya harus peduli terhadap dampak yang ditimbulkan kejahatan ini dan berupaya serius untuk menanggulanginya.

---

[126] Nur Khalimatus Sa'diyah,. *Op cit*.
[127] *Ibid.,*

Pencegahan terhadap tindak pidana *hacker* dan *cracker*, harus mencakup semua akses ilegal atau akses ke internet yang merugikan pihak lain. Akses iilegal ini meliputi akses tanpa izin, merusak data atau program komputer, melakukan sabotase untu menghilangkan sistem atau jaringan komputer tanpa izin, serta memata-matai komputer.

4. Keresahan masyarakat pengguna komputer

Menurut TB. Ronny R, Nitibaskara, kejahatan atau crime tidak dapat dipisahkan dari lima faktor yang saling berhubungan, yaitu:[128]

a) Pelaku kejahatan

Dalam hal pelaku kejahatan hacking dan cracking, karakter subjek hukum berbeda dari pelakunya. Pelaku tampaknya memiliki keunikan tersendiri, yang belum tertampung dalam konsep-konsep atau teori konvensional mengenai tindak kejahatan.

b) Modus operandi kejahatan

Bahwa suatu modus operandi *hacking* dan *cracking* sangat berbeda dari tindak kejahatan konvensional, yang paling mencolok dari perbedaan tersebut antara lain locus delicti atau tempat kejadian perkara karena sangat sulit melokalisir jaringan internet.

c) Korban kejahatan

Korban *hacking* dan *cracking* tidak selalu dalam bentuk dapat dilihat atau tangible melainkan juga tidak terlihat intangible karena tempat tinggal dan kewarganegaraan korban yang tidak selalu sama

[128] *Ibid.,*

dengan *hacker* dan *cracker*, maka penegak hukum menghadapi masalah jauh lebih kompleks lagi.

d) Reaksi sosial atas kejahatan

Reaksi sosial atas suatu tindak kejahatan jauh lebih terukur daripada yang terjadi pada kasus *hacking* dan *cracking*. Misalnya, reaksi masyarakat terhadap perampok atau pencuri yang tertangkap berupa penghakiman masa. Sebaliknya, segmen masyarakat yang bereaksi atas suatu tindakan cracking tidak sebesar pada kasus konvensional. Namun demikian dampak *hacking* dan *cracking* lebih kecil dibandingkan dengan kejahatan-kejahatan konvensional.[129]

e) Hukum

Undang-undang dan perangkat hukum serta aturan lain yang bersifat empirik hingga saat ini masih banyak diantaranya yang bersandar pada yurisprudensi. Sebaliknya, Undang-undang nomor 19 tahun 2016 tentang perubahan atas Undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik dalam perkembangan kerangka hukum yang ada kalah pesat dibandingkan dengan perkembangan kejahatan yang terjadi

5. Dampak keamanan cracking terhadap keamanan dalam negeri

Ketidaksiapan Indonesia dalam mengantisipasi perkembangan teknologi informasi dalam bentuk struktur maupun infrastruktur hukum bisa berakibat buruk

[129] *Ibid.,*

dan bukan tidak mungkin ancamannya adalah kerawanan sosial dan politik yang ditimbulkan oleh individu individu yang berperilaku menyimpang. Motif para *hacker* dan *cracker* bukan hanya *money oriented*, tetapi juga melemparkan isu-isu yang meresahkan, memanipulasi simbol-simbol kenegaraan dan partai politik dengan tujuan untuk mengacaukan keadaan agar tidak tercipta suasana yang kondusif.

Selain ingin meraih keuntungan secara finansial dari kegiatan kegiatan *hacking* dan *cracking* tersebut, mereka juga berusaha merusak situs-situs perbankan, kartu kredit, toko-toko yang menawarkan barang secara online, lembaga-lembaga keuangan, bursa efek, kurs valuta asing, dengan maksud terjadinya kekacauan dalam bidang perdagangan.[130]

D. Konstruksi *Hacking* dan *Cracking* Sebagai Kejahatan *Cybercrime*

Hacking merupakan salah satu kegiatan yang bersifat negatif tersebut. Meskipun pada awalnya *hacking* memiliki tujuan mulia, yaitu untuk memperbaiki sistem keamanan yang telah dibangun dan memperkuatnya, tetapi dalam perkembangannya *hacking* digunakan untuk keperluan-keperluan lainya yang bersifat merugikan. Hal ini tak lepas dari penggunaan internet yang semakin meluas sehingga penyalahgunaan kemampuan *hacking* juga mengikuti luasnya pemanfaatan internet. Dapat diketahui bahwa tahap-tahap seseorang dalam melakukan hacking yaitu sebagai berikut:

1) mencari sistem yang hendak dimasuki;
2) menyusup dan menyadap password;

[130] *Ibid.,*

3) menjelajahi sistem komputer;
4) membuat backdoor dan menghilangkan jejak.

Tidak setiap tahap dari *hacking* dapat disebut sebagai kejahatan. Tahap pertama dari *hacking* tidak dapat disebut sebagai kejahatan karena belum dapat dikatakan ada bahaya serius yang mengancam. Tahap kedua sampai keempat, dapat disebut sebagai kejahatan. Tahap kedua merupakan tahap yang paling ringan karena dalam tahap ini hanya bersifat masuk atau menyusup dan belum ada tindakan destruktif. Tahap ketiga dan keempat sudah mengandung unsur destruktif sehingga akibat yang ditimbulkan lebih buruk dibandingkan dengan tahap kedua.

Tahap kedua sampai keempat merupakan kejahatan, hal ini disebabkan beberapa hal, yaitu:

1) memasuki ruang privat pada situs orang lain bukanlah perbuatan terpuji. Sebuah situs dalam proses komunikasi dengan pihak lain (pihak yang mengakses) sudah menyaksikan tempat publik itu. Bagaimana ruang publik itu dikelola dan disajikan, merupakan urusan pengelola disitus. Pihak pengakses dapat memberikan saran ataupun kritik terhadap apa yang disajikan itu pada tempat atau alamat yang disediakan oleh pengelola situs. Menggangu privasi orang merupakan pelanggaran terhadap hak asasi orang lain sehingga menyusup, apalagi dilakukan secara diam-diam betul-betul merupakan tindakan yang tidak didasarkan pada moral yang baik. Jika situs yang disusupi itu adalah milik sebuah instansi pemerintah yang vital, sepeti militer yang menyimpan data-data penting atau rahasia bahkan

sangat rahasia mengenai negara, maka masuk atau menyusup kedalam situ situ tanpa izin merupakan tindakan mata-mata. Dalam konstruksi hukum pidana, tindakan menyusup ini dapat dikategorikan sebagai tindakan memata- matai.

2) Menjelajahi daerah atau ruang milik orang lain tanpa izin merupakan kejahatan karena mengganggu privasi pemilik daerah itu. Jika penjelajahan itu dilakukan dan disertai dengan tindakan destrtuktif, misalnya mengubah tampilan atau frontpage dari suatu situs sudah merupakan perbuatan mengacaukan ketertiban umum. Tindakan merusak milik orang lain dalam konstruksi hukum pidana sudah merupakan tindak pidana. Meskipun tindakan itu membawa akibat dalam pelayanan publik di dunia maya, tetapi kerugian yang timbul dirasakan oleh orang-orang yang ada di dunia nyata. Tindakan *hacker* yang berusaha untuk mendapatkan akses yang lebih tinggi merupakan tindakan yang dapat dikategorikan sebagai tindakan pengambilalihan kekuasaan (kudeta) terhadap kekuasaan yang hanya dimiliki oleh administrator sistem. Dengan menjadi superuser berarti cracker menjadi penguasa jaringan komputer atau situs yang dimasukinya itu.
3) meninggalkan tempat yang telah dimasuki apalagi disertai dengan tindakan menghapus *log file* atau data-data penting lai dalam usaha meninggalkan jejak menunjukan tindakan yang dilakukan *hacker* merupakan tindakan yang tidak bertanggungjawab. Tidak ada kejahatan yang menyatakan dirinya bertanggung jawab terhadap perbuatan yang dilakukannya. Secara

etis tindakan tidak bertanggung jawab ini bertentangan dengan tuntutan moral yang menekankan kejujuran dan pertanggungjawaban.

Agar dapat disebut atau dikategorikan sebagai kejahatan, maka harus mmenuhi beberapa karakteristik dari tindak pidana, yaitu:

a) Bertentangan dengan atau merugikan kepentingan umum (*a public wrong*).

Dilihat dari kriteria ini, maka tindakan *hacking* yang dilakukan oleh cracker sangat bertentangan dan merugikan kepentingan umum bahkan kepentungan pribadi. Seorang cracker yang menyerang situs yang menyediakan pelayanan publik atau menyediakan data-data yang diperuntukan bagi publik sudah barang tentu merugikan pengakses situs-situs, dalam hal ini tidak hanya pemerintah atau perusahaan yang dirugikan (sebagai penyelanggara pelayanan umum) tetapi juga merugikan kepentingan pengakses. Demikian juga dengan situs yang dikelola secara pribadi, jika di-hack maka akan mengganggu kepentingan dari pemilik situs-situs secara pribadi.

b) Bertentangan dengan moral masyarakat (*a moral wrong*)

Tidaklah mudah untuk menentukan dasar moral apa yang dipakai sebagai pertimbangan dalam memutuskan suatu perbuatan sebagai kejahatan atau tidak. Dalam hal ini dasar moral yang dipakai tentunya dapat diambil dari kehidupan masyarakat sekitar atau dimana perbuatan itu ada atau terjadi (yang berarti kehidupan dalam alam nyata) dan ketentuan- ketentuan moral yang dipakai atau digunakan dalam kehidupan para netizen (dalam hal ini moral dalam kehidupan para netizen). Para netizen umumnya mengakui bahwa meng-hack sebuah situs

merupakan tindakan yang tidak baik apalagi jika hacking itu dilakukan terhadap situs-situs pendidikan, penelitian dan pelayanan umum.

E. Pengaturan Hukum Pidana Terhadap *Hacking* dan *Cracking* Menurut Kitab Undang-undang Hukum Pidana (KUHP)

Dalam hukum pidana terdapat pendekatan dalam menerapkan suatu ketentuan pidana, yang biasa dikenal dengan istilah *interpretasi* atau penafsiran. Tidak akan diuraikan secara menyeluruh mengenai penafsiran, namun secara lebih khusus akan dibahas mengenai penafsiran *ekstentif*. Penafsiran *ekstensif* adalah untuk memperluas pengertian dari suatu istilah yang berbeda dengan pengertiannya yang digunakan dalam istilah sehari-hari. Mengenai penggunaan cara penafsiran ini, sering terjadi perbedaan pendapat dimana para ahli karena sukar memberi batas bagi perluasan tersebut. Hal ini menjadi perhatian karena analogi juga dikatakan sebagai perluasan pengertian atau perluasan cakupan ketentuan suatu peraturan yang pada umumnya analogi tidak diperbolehkan dalam hukum pidana.

Menggunakan analogi berarti menganggap sesuatu sebagai termasuk dalam pengertian dari suatu ketentuan undang-undang hukum pidana, karena sesuatu itu banyak sekali kemiripannya atau kesamaannya dengan ketentuan tersebut.Contoh terkenal mengenai penerapan analogi adalah kasus pencurian aliran listrik. Yang menjadi persoalan adalah, apakah aliran listrik dianggap sebagai “barang” dan apakah terjadi tindakan “mengambil”.*Hooge Raad* (seorang mahkamah agung di negara Belanda) telah memutuskan bahwa aliran listrik termasuk kedalam pengertian “barang” dan dengan demikian terjadi

"pengambilan" sesuai dengan istilah yang digunakan dalam pasal 362 KUHP, walaupun pada kenyataannya yang terjadi adalah penyalurannya. Pertimbangan dari Hooge Raad adalah bahwa maksud dari pasal 362 adalah untuk melindungi harta orang lain, tanpa merumuskan apa yang dimaksud dengan "barang" itu sendiri. (arrest HR tanggal 23 Mei 1921 W 10728).[131]

Penafsiran ekstensif berbeda dengan analogi. Menurut Wirjono perbedaan antara penafsiran ekstensif dengan analogi adalah :

> Orang masih ada dibidang penafsiran ekstensif apabila dari kata-kata suatu peraturan hukum tidak terlihat, tetapi dengan suatu cara pikiran itu disimpulkan, bahwa suatu kejadian atau peristiwa tertentu dimaksudkan turut teratur juga. Sedangkan analogi terjadi apabila suatu penafsiran disimpulan bahwa suatu kejadian atau peristiwa tertentu tidak turut diatur dalam suatu peraturan hukum, namun tetap saja dianggap diliputi oleh peraturan itu.[132]

Penerapan KUHP terhadap tindak pidana *hacking* maupun *cracking* memerlukan pemilahan, perbuatan mana yang substansinya hampir sama dengan rumusan tindak pidana biasa dalam KUHP, rumusan perbuatan yang dimaksud yakni:

Dalam aktivitas perbuatan *hacking* adalah sebuah aktivitas dimana untuk melakukan akses sistem komputer secara melawan hukum atau ilegal dalam dunia internet. Sedangkan rumusan dalam KUHP adalah memasuki atau melintas batas wilayah secara tidak sah, hal ini seperti yang dimaksud dalam pasal 167 KUHP yakni:

1. Barangsiapa memaksa masuk kedalam rumah, ruangan, atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum

---

[131] E.Y. Kanter dan S.R. Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya,* Jakarta, Alumni AHM-PTHM, 1982, halaman.76-77

[132] Wirjono Prodjodikoro, *Asas-asas Hukum Pidana di Indonesia*, Jakarta, PT. Eresco, 1969 , sebagaimana dikutip oleh E.Y. Kanter dan S.R. Sianturi halaman. 68

atau berada disitu dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana pejara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

2. Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jahat palsu atau barangsiapa tidak setahu yang berhak lebih dahulu serta bukan karena kekhilafan masuk dan kedapatan disitu pada waktu malam dianggap memaksa masuk.
3. Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang diancam dengan pidana penjara paling lama satu tahun empat bulan.
4. Pidana tersebut dalam ayat 1 dan 3 dapat ditambah sepertiga jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu.

Sebagaimana diketahui, *konvergensi* teknologi (komputer, komunikasi, dan informasi) yang terwujud dalam bentuk internet, dimana isu privacy merupakan suatu hal yang tidak bisa ditawar lagi. Jika terjadi suatu penyusupan terhadap suatu sistem komputer dan disaat yang bersamaan tindakan tersebut telah terdeteksi oleh pemilik sistem, tindakan tersebut dapat dikategorikan sebagai suatu pelanggaran atau kejahatan jika dampak yang ditimbulkan dapat menimbulkan kerugian kepada orang lain. Unsur-unsur yang dapat ditemukan dalam pasal 167 KUHP, adalah:

1. Unsur Subjektif : Unsur subjektif yang dimaksud dalam pasal 167 KUHP adalah tiada kekhilafan atau ringkasanya adanya suatu kesengajaan dalam melakukan perbuatan tersebut. Dalam KUHP, perbuatan tersebut dilakukan dengan kesengajaan dimana pelaku diketahui dan setelah diperingati tidak diindahkan oleh yang bersangkutan. Dari rumusan tersebut dapat ditarik suatu kesimpulan bahwa adanya suatu kesengajaan dalam tindakan tersebut.Jika KUHP diterapkan dalam tindak pidana *hacking* ini, sifat kesengajaan dari

perbuatan tersebut perlu dibuktikan di sidang pengadilan dan jika terbukti maka *hacker* atuapun *cracker* baru dapat dipidana.

2. Unsur Objektif : Memasuki wilayah dalam hal ini wilayah fisik seperti rumah, ruangan atau pekarangan tertutup.Sifat fisik ini yang membatasi aturan pidana KUHP dapat diterapkam, *cyberspace* bukanlah wilayah fisik seperti yang dibayangkan pada umumnya.Oleh sebab itu, perlu adanya perubahan makna supaya tidak ada lagi sifat fisik dari *cyberspace* yang dijadikan perdebatan.*Cyberspace* yang bersifat tidak nyata ini dapat menjadikan tindakan yang besifat fisik tidak lagi dijadikan sandaran bahwa *hacking* telah melakukan tindak pidana. Unsur barangsiapa tetap dijadikan patokan, hanya saja cara yang dilakukan tidak lagi langsung pada objek fisik, tindakan yang dimaksud disini berupa suatu jejak elektronik yang berisikan *log file*, angka atau data matematis yang mengindikasikan telah berlangsung aktivitas elektronis.

Dalam perbuatan *cracking,* yang dimaksud adalah melakukan akses sistem komputer secara ilegal atau melawan hukum yang menyebabkan rusaknya sebuah sistem komputer yang diakses tidak dapat di operasikan lagi *(down)*. Apabila dilihat dari substansi perbuatannya dan efek yang ditimbulkan, perbuatan *cracking* tersirat dalam KUHP yang mengatur perihal perusakan atau penghancuran tersebut, yaitu dalam pasal 406 ayat 1 KUHP, yang dirumuskan sebagai berikut:[133]

[133] Andi Hamzah, *Hukum Acara Pidana Indonesia*, Jakarta, Sinar Grafika, 2005, halaman 5.

> Barangsiapa dengan sngaja melawan hukum, menghancurkan, merusakan, membuat tidak dapat dipakai atau menghilangkan barang sesuatu baik seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara dua tahun delapan bulan penjara atau denda paling banyak empat ribu lima ratus rupiah.

Dalam pasal 406 ayat 1 KUHP tersebut, Menurut Andi Hamzah apabila dikaitkan dengan perbuatan *cracking*, dapat ditarik penjelasan sebagai berikut:

1. Pengertian *menghancurkan*, maka perbuatan menghancurkan jika dikaitkan dengan *cracking* adalah suatu penghancurkan hardisk, flashdisk, jaringan komputer, website, sisstem informasi dan sejenisnya yang berisi data atau program komputer yang mana program didalamnya menjadi hancur dan tidak dapat di manfaat kan lagi.
2. Pengertian *merusak*, Jika Dikaitkan dengan *cracking*, perbuatan merusak adalah suatu perbuatan merusak data yang terdapat dalam suatu media penyimpanan elektronik atau sejenisnya, menghapus data, mengacak-acak data didalamnya, membuat cacat didalamnya, atau menambahkan data baru.
3. Pengertian *membuat tidak dapat lagi,* Jika dikaitkan dengan *cracking, membuat tidak dapat dipakai lagi* adalah suatu perbuatanyang dilakukan sedemikian rupa sehingga data dalam suatu sistem komputer yang seharusnya dapat di manfaatkan sesuai dengan fungsinya, menjadi tidak dapat lagi digunakan karena telah dihapus, dirusak atau dikacakan.
4. Penegertian *menghilangkan,* Jika dikaitkan dengan *cracking*, *menghilangkan* adalah suatu perbuatan menghilangkan atau menghapus data atau program

yang tersimpan dalam suatu sistem atau sejenisnya sehingga mengakibatkan suatu data atau informasi yang disimpan menjadi terhapus sama sekali.[134]

Dari konstruksi hukum yang dipaparkan oleh Andi Hamzah , terlihat adanya penyesuaian antara pengertian *pengrusakan barang* dengan suatu pengertian *pengrusakan data atau program komputer*, yag pada konsepnya perbuatan tersebut menyebabkan fungsi dari data, informasi atau program menjadi terganggu atau bahkan mengalami kerusakan sistem *(System Denied)*.

F. Yurisdiksi Dalam Penegakan Hukum Terhadap kejahatan *Hacking* dan *Cracking*

Kejahatan dalam ruang *cyber* bersifat transnasional dimana kejahatan ini dapat terjadi secara lintas batas wilayah negara tetapi akibatnya memiliki implikasi hukum di Indonesia. Dengan demikian perlu adanya penentuan yurisdiksi apabila *cybercrime* yang terjadi nantinya bersifat lintas batas negara. Yurisdiksi adalah kekuasaan atau kompensasi hukum negara terhadap orang, benda ataupun peristiwa hukum. Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak campur tangan. Yurisdiksi merupakan suatu bentuk kedaulatan vital dan sentral yang dapat mengubah, menciptakan, atau mengakhiri suatu hubungna atau kewajiban hukum.[135]

---

[134] Edmon Makarim, *Pengantar Hukum Telematika-suatu kompilasi kajian*, PT. Raja Grafindo Persada, Jakarta, 2005, halaman 433

[135] Didik M.Arief Mansur, *Cyber Law-Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005, Halaman 30

1. *Locus Delicti,* Dalam Penentuan Yurisdiksi Tindak Pidana *Hacking* dan *Cracking* dalam KUHP

Dalam tindak pidana *hacking* maupun *cracking,* Penentuan yurisdiksi atau kewenangan mengadili merupakan suatu persoalan yang haruslah memiliki suatu landasan hukum, dimana dalam menentukan kewenangan mengadili suatu tindak pidana didasarkan pada *locus delicti*. Dimana tersirat dalam pasal 84 KUHAP yang berbunyi "Pengadilan Negeri berwenang mengadili segala perkara tindak pidana yang dilakukan didaerah hukumnya". Berdasarkan teori, bahwa *locus delicti* dapat di artikan semua tempat, baik tempat dimana seorang pelaku itu telah melakukan sendiri perbuatannya yang dilarang oleh undang-undang maupun tempat dimana alat yang dipergunakannya itu telah menimbulkan akibat. Apabila *locus delicti* tindak pidana *hacking* dan *cracking* terjadi di wilayah hukum Indonesia maka hal itu menyangkut kewenangan relatif. Namun apabila *locus delicti* tindak pidana *hacking* terjadi di luar wilayah Indonesia maka hal ini menyangkut yurisdiksi. Berikut akan paparkan bagaimana tindak pidana *hacking* dapat diadili apakah akan diadili berdasarkan yurisdiksi Indonesia ataukah berdasarkan yurisdiksi negara yang bersangkutan.

Locus delicti berada di Indonesia. Jika tempat pelaku berbuat, alat kejahatan dan akibat yang dirugikan oleh tindak pidana *hacking* berada dalam wilayah Indonesia maka berdasarkan asas teritorial yang terdapat dalam Pasal 2 dan 3 KUHP merupakan Yurisdiksi Indonesia untuk mengadili pelaku *hacking* tersebut. Dimana tindak pidana *hacking* tersebut telah diatur dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor

11 Tahun 2008 Tentang Informasi dan Transaksi elektronik. Yurisdiksi dengan prinsip teritorial, bahwa setiap negara mempunyai yurisdiksi terhadap kejahatan-kejahatan yang dilakukan di dalam wilayahnya terhadap setiap orang dan setiap benda yang berada di dalam wilayahnya. Undang-undang Pidana berlaku terhadap setiap orang yang bersalah telah melakukan tindak pidana di dalam wilayah suatu negara.

Pasal 2 KUHP menyatakan:

> Ketentuan Pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu tindak pidana di Indonesia.

Pasal 3 KUHP menyatakan:

> Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi setiap orang yang diluar wilayah Indonesia melakukan tindak pidana di dalam kendaraan air indonesia.

Asas teritorial sebagaimana telah diatur dalam Pasal 2 dan Pasal 3 KUHP ternyata telah diperluas lagi dalam ketentuan Undang- Undang nomor 4 tahun 1976 tentang perubahan dan penambahan beberapa pasal dalam KUHP bertalian dengan perluasan berlakunya ketentuan perundang-undangan pidana, kejahatan penerbangan, dan kejahatan terhadap sarana/prasarana penerbangan seperti yang diatur dalam Pasal 1 (mengenai penambahan ketentuan dalam Pasal 3 KUHP) yang menyatakan bahwa: ”Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi setiap orang yang di luar Wilayah Indonesia melakukan tindak pidana di dalam kendaraan air atau pesawat udara Indonesia”. Berlakunya asas ini didasarkan pada asas kedaulatan suatu negara, sehingga setiap orang baik yang secara tetap maupun untuk sementara berada dalam wilayah negara tersebut,

harus menaati dan menundukkan diri pada segala perundang-undangan yang berlaku di negara tersebut.

Berdasarkan hal tersebut di atas maka tindak pidana *hacking* maupun *cracking* yang dilakukan di dalam wilayah Indonesia terhadap sistem elektronik di Indonesia dapat diadili menurut hukum yang berlaku di Indonesia. Contoh: seorang *hacker* yang berada di Kota Jambi melakukan *hacking* sebuah website dimana terdaftar pada server di Jakarta. Dalam menentukan kewenangan mengadili dalam contoh tersebut maka ditentukan kewenangan relatif dalam penentuan mengadili tindak pidana *hacking* tersebut.

Locus delicti berada di luar wilayah Indonesia Jika dalam hal tindak pidana *hacking* terjadi di luar wilayah Indonesia apakah itu tempat perbuatan tindak pidana, tempat alat yang digunakan berfungsi atau akibat yang terjadi salah satunya berada diluar negeri. Maka dalam hal ini hukum pidana telah mengatur bagaimana tindak pidana *hacking* dapat diadili menurut undang- undang Indonesia sesuai asas-asas yang menjadi dasar menentukan yurisdiksi yaitu asas nasional aktif, asas pelindungan dan asas universal. Maka dalam menentukan yurisdiksi dapat kita lihat dalam beberapa asas yaitu:

1) Yurisdiksi berdasarkan asas personal atau asas nasional aktif

Yurisdiksi berdasarkan asas personal atau asas nasional aktif atau juga disebut *actieve persoonlijkheidsstelsel*. Asas ini memungkinkan penegak hukum Indonesia untuk melaksanakan yurisdiksinya dan memaksakan hukum pidana nasionalnya terhadap warga negaranya yang melakukan tindak pidana di luar wilayah Indonesia. Undang-undang Pidana Indonesia tetap diberlakukan terhadap

warga negaranya dimana pun mereka itu berada, bahkan juga seandainya mereka itu berada diluar negeri (Pasal 5 dan 7 KUHP).

Pasal 5 KUHP menyatakan bahwa:

(1) Ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi warga negara yang di luar Indonesia melakukan:
    1. salah satu kejahatan tersebut dalam Bab I dan II Buku kedua dan Pasal-Pasal 160, 161, 240, 279, 450, dan 451.
    2. salah satu perbuatan yang oleh suatu ketentuan pidana perundang-undangan Indonesia dipandang sebagai kejahatan, sedangkan menurut perundang-undangan negara dimana perbuatan dilakukan diancam dengan pidana.
(2) penuntutan perkara sebagaimana dimaksud dalam butir 2 dapat dilakukan juga jika tertuduh menjadi warga negara sesudah melakukan perbuatan.

Pasal 7 KUHP menyatakan bahwa:

Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi setiap pejabat yang diluar Indonesia melakukan salah satu tindak pidana sebagaimana dimaksudkan dalam Bab XXVIII Buku Kedua

2) Yurisdiksi berdasarkan asas perlindungan atau asas nasional pasif

Berdasarkan asas perlindungan atau asas nasional pasif atau juga disebut *passief nationaliteits-beginsel*., Indonesia dapat melaksanakan yurisdiksinya terhadap warga negara asing yang melakukan kejahatan di luar negeri yang diduga dapat mengancam kepentingan keamanan, integritas, dan kemerdekaan Indonesia. Berlakunya Undang-undang Pidana Indonesia berlaku bagi setiap orang tanpa memandang kebangsaan orang-orang tersebut yang berada diluar negeri dimana tindak pidana yang dilakukannya membahayakan kepentingan-kepentingan nasional yang perlu mendapat perlindungan (Pasal 4 dan 8 KUHP).

Pasal 4 KUHP menyatakan bahwa:

Ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan di luar Indonesia:

1. salah satu kejahatan berdasarkan pasal-pasal 104, 106, 107,108,dan 131;
2. suatu kejahatan mengenai mata uang atau uang kertas yang dikeluarkan oleh negara atau bank, ataupun mengenai meterai yang dikeluarkan dan merek yang digunakan oleh Pemerintah Indonesia;
3. pemalsuan surat hutang atau sertifikat hutang atas tanggungan Indonesia, atas tanggungan suatu daerah atau bagian daerah Indonesia, termasuk pula pemalsuan talon, tanda dividen atau tanda bunga, yang mengikuti surat atau sertifikat itu, dan tanda yang dikeluarkan sebagai pengganti surat tersebut, atau menggunakan surat-surat tersebut di atas, yang palsu atau dipalsukan, seolah-olah asli dan tidak dipalsu;
4. salah satu kejahatan yang tersebut dalam pasal-pasal 438, 444 sampai dengan 446 tentang pembajakan laut dan pasal 447 tentang penyerahan kendaraan air kepada kekuasaan bajak laut dan pasal 479 huruf j tentang penguasaan pesawat udara secara melawan hukum, pasal 479 huruf I, m, n, dan o tentang kejahatan yang mengancam keselamatan penerbangan sipil.

Pasal 8 KUHP menyatakan bahwa:

> Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi nahkoda dan penumpang perahu Indonesia, yang di luar Indonesia, sekalipun di luar perahu, melakukan salah satu tindak pidana sebagaimana dimaksudkan dalam Bab XXIX Buku Kedua, dan Bab IX Buku Ketiga, begitu pula yang tersebut dalam peraturan mengenai surat laut dan pas kapal Indonesia, maupun dalam Ordonansi Perkapalan.

Berdasakan yurisdiksi ini, kejahatan-kejahatan yang dilakukan oleh warga negara asing di luar negeri yang dapat membahayakan kepentingan nasional dapat diadili menurut hukum di Indonesia yang pengaturannya terdapat dalam Pasal 4 dan 8 KUHP . Namun aturan ini tidak menyangkut tentang tindak pidana *hacking* dimana tindak pidana *hacking* tidak diatur dalam KUHP.

3) Yurisdiksi berdasarkan asas universal

Bahwa setiap negara mempunyai yurisdiksi untuk mengadili tindak kejahatan tertentu. Wewenang untuk melaksanakan asas universal dimiliki tiap negara tanpa melihat siapa pelakunya dan tanpa melihat dimana tindak pidana itu dilakukan. Persyaratan mengenai tindak pidana tersebut sebagai serious crime harus terpenuhi sehingga tindak pidana itu memiliki karakter membahayakan masyarakat internasional. Dengan demikian ada dasar pembenaran bahwa pelaksanaan yurisdiksinya tidak diserahkan pada satu negara tertentu saja tetapi menjadi hak setiap negara secara universal.

Pasal 4 ke-2 dan ke-4 KUHP dinyatakan bahwa:

> Ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan di luar Indonesia.
> 1. suatu kejahatan mengenai mata uang atau uang kertas yang dikeluarkan oleh negara atau bank, ataupun mengenai meterai yang dikeluarkan dan merek yang digunakan oleh Pemerintah Indonesia.
> 2. salah satu kejahatan yang tersebut dalam pasal-pasal 438, 444 sampai dengan 446 tentang pembajakan laut dan pasal 447 tentang penyerahan kendaraan air kepada kekuasaan bajak laut dan pasal 479 huruf j tentang penguasaan pesawat udara secara melawan hukum, pasal 479 huruf I, m, n, dan o tentang kejahatan yang mengancam keselamatan penerbangan sipil.

Asas persamaan atau universal yaitu setiap negara mempunyai kewajiban untuk turut serta dalam usaha memelihara keamanan dan ketertiban dunia dengan negara-negara lain (Pasal 4 angka 2 dan 4 serta Pasal 438, 444,445 dan 446 KUHP). Asas ini selayaknya memperoleh perhatian khusus terkait penanganan hukum kasus-kasus *cybercrime* terkhusus tindak pidana *hacking* dan *cracking*. Asas ini disebut juga sebagai *universal interest jurisdiction*. Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para

pelaku kejahatan pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (*crimes against humanity*), misalnya penyiksaan, genosida pembajakan udara dan lain-lain. Asas tersebut kiranya juga digunakan untuk menangani *cybercrime* mengingat *cybercrime* merupakan kejahatan transnasional yang memiliki dampak yang serius bagi masyarakat internasional. Dalam prakteknya, Indonesia dalam menangani masalah *cybercrime* lebih merujuk kepada asas teritorial dimana memang negara mutlak menindak para *hacker* dan *cracker* yang melakukan kejahatannya di dalam wilayah Indonesia. Baik itu warga negara Indonesia, maupun warga negara asing asalkan mereka berada dalam wilayah Indonesia saat melakukan kejahatannya.

Berkaitan dengan asas-asas yurisdiksi lain bahwa tidak begitu saja ditinggalkan, akan tetapi penegak hukum di Indonesia memiliki keterbatasan-keterbatasan jika tindak pidana hacking dilakukan di luar wilayah Indonesia dimana terdapat peraturan-peraturan internasional dalam penanggulangan *cybercrime*. Perlu adanya perjanjian kerjasama keamanan dengan negara-negra lain termasuk perjanjian ekstradisi dengan berbagai negara untuk dapat mengadili pelaku tindak pidana.

2. Aspek Yurisdiksi pada Tindak Pidana *Hacking* dan *Cracking* Menurut Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik

Sebagai bagian dari dunia internasional Indonesia turut serta dalam penanggulangan kejahatan yang bersifat transnasional. Kejahatan transnasional

merupakan suatu kejahatan dimana ada atau tidaknya unsur asing, adanya kesamaan pandangan bahwa suatu perbuatan memiliki dampak negatif bagi dua negara atau lebih, serta penggunaan sarana dan prasarana yang melampau batas teritorial. Berdasarkan hal tersebut maka Indonesia menindaklanjuti kerjasama internasional dalam menanggulangi kejahatan transnasional baik itu kerjasama bilateral maupun multilateral serta kerjasama secara regional dalam lingkup ASEAN dan PBB. Berdasarkan hal tersebut di atas Indonesia telah membuat peraturan perundang-undangan dimana yurisdiksi dalam kejahatan transnasional telah diatur khususnya *cybercrime* yaitu terdapat dalam Pasal 2 dan Pasal 37 Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik.

a) Pasal 2 Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik disebutkan bahwa:

> Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagai mana diatur dalam Undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Dalam pasal penjelasan Undang-undang ini pada Pasal 2 diberi penjelasan bahwa Undang-undang ini memiliki jangkauan Yurisdiksi tidak semata-mata untuk tindak pidana yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk tindak pidana yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing

yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik bersifat lintas teritorial atau universal.

Dengan pengertian tersebut maka tempat kejadian atau *locus delicti* tindak pidana *hacking* tidak terbatas dalam wilayah teritorial Indonesia akan tetapi juga dapat berada diluar wilayah teritotial Indonesia dimana tindak pidana tersebut mengakibatkan kerugian di wilayah Indonesia. Yang dimaksud dengan ”merugikan kepentingan Indonesia” adalah meliputi tapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, warga negara, serta badan hukum Indonesia.

b) Pasal 37 Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik disebutkan bahwa:

> Setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

Hal yang berkaitan dengan yurisdiksi juga diperkuat dengan Pasal 37 dimana hacking sebagai salah satu tindak kejahatan internet/*cybercrime* diatur pemberlakuannya. *Hacking* dan *cracking* sebagai salah satu *cybercrime* dan dapat merupakan tindakan awal untuk *cybercrime* lainnya seperti halnya penyadapan/intersepsi, *hacking*, *cracking, carding, virusing/attacking* dan manipulasi data otentik telah diatur dalam Pasal 27 sampai Pasal 36 Undang-

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik.

Undang–undang ini berlaku secara luas tidak terbatas pada para pelaku yang berada di wilayah hukum Indonesia tetapi juga terhadap pelaku yang berada di luar negeri atau di luar wilayah hukum Indonesia dimana dampak *cybercrime* tersebut merugikan Indonesia. Hal tersebut dapat dikaitkan dengan teori *locus delicti* dimana tempat kejadian peristiwa tindak pidana walaupun berada di luar teritorial Indonesia akan tetapi memiliki dampak terhadap sistem elektronik di wilayah Indonesia maka pelaku *hacking* ataupun *cracking* dapat dijerat dengan pasal ini. Dengan demikian bahwa tindak pidana hacking sebagai salah satu kejahatan internet/*cybercrime* baik bagi warga negara Indonesia maupun warga negara asing, baik dilakukan di dalam wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia dimana tindak pidana tersebut menimbulkan dampak yang merugikan di Indonesia.

Berdasarkan Pasal 2 dan pasal 37 penjelasan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik pada dasarnya tetap dianut asas-asas ruang berlakunya hukum pidana dalam KUHP yaitu didasarkan pada asas teritorial (pasal 2-5 KUHP), asas personal/nasional aktif (pasal 7 KUHP), dan asas universal (pasal 8 KUHP), hanya ada perubahan dan perkembangan formulasinya yaitu:

a) Memuat ketentuan tentang lingkup yurisdiksi yang bersifat transnasional dan internasional serta memuat ketentuan khusus terhadap tindak pidana teknologi informasi.
b) Subjek hukum tidak hanya terhadap perorangan baik warga negara Indonesia ataupun warga negara asing yang memiliki akibat hukum di Indonesia tetapi juga terhadap badan hukum asing (koorporasi)

Menurut Masaki Hamano sebagaimana dikutip oleh Barda Nawawi Arief Ada tiga lingkup yurisdiksi di ruang maya (*cyberspace*), yang dimiliki suatu negara berkenaan dengan penetapan dan pelaksanaan pengawasan terhadap setiap peristiwa, setiap orang dan setiap benda. Ketiga katagori yurisdiksi tersebut, yaitu:[136]

a) Yurisdiksi Legislatif (*legislatif jurisdiction atau jurisdiction to prescribe*);
b) Yurisdiksi Yudisial (*judicial jurisdiction atau jurisdiction to adjudicate*);
c) Yurisdiksi Eksekutif (*executive jurisdiction atau jurisdiction to enforce*).

Berdasarkan ketiga katagori yurisdiksi menurut Masaki Hamano di atas perbuatan yang dapat menimbulkan masalah dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik ketika warga negara Indonesia melakukan tindak pidana diluar Indonesia (asas personal/nasional aktif) tanpa akibatnya dirasakan di Indonesia. Hal tersebut sangat terkait dengan masalah yurisdiksi judisial (kewenangan mengadili atau menerapkan hukum) dan yurisdiksi eksekutif (kewenangan melaksanakan putusan) karena masalah

[136] Masaki Hamano,"*Comparative Study in the Approach to Jurisdiction in Cyberspace"* Chapter: The Principle of Jurisdiction,hal.1. lihat dalam Barda Nawawi Arief, Tindak Pidana Mayantara, Op.Cit.,Halaman .27-28.

yurisdiksi judisial/adjudikasi dan yurisdiksi eksekutif sangat terkait dengan kedaulatan wilayah dan kedaulatan hukum masing-masing Negara, karena konstitusi suatu negara tidak dapat dipaksakan kepada negara lain karena dapat bertentangan dengan kedaulatan dan konstitusi negara lain, oleh karena itu hanya berlaku di negara yang bersangkutan saja, sehingga dibutuhkan kesepakatan Internasional dan kerjasama dengan negara-negara lain dalam menanggulangi tindak pidana teknologi informasi khususny *hacking* dan *cracking*.

BAB IV
PENEGAKAN HUKUM PIDANA TERHADAP PELAKU AKSES SISTEM KOMPUTER SECARA ILEGAL (*HACKING)* DAN MENIMBULKAN KERUSAKAN (*CRACKING)* DALAM DUNIA MAYA (*CYBERCRIME*)

A. Penegakan Hukum pidana Terhadap Pelaku Kejahatan *hacking (hacker)* dan *Cracking (cracker)*

Pesatnya teknologi informasi melaui internet telah mengubah aktivitas-aktivitas kehidupan yang semula perlu dilakukan secara kontak fisik, kini dengan menggunakan media *cyberspace*, aktivitas keseharian dapat dilakukan secara vitual atau maya. Masalah rumit yang dihadapi penegak hukum saat ini adalah bagaimana menjaring pelaku *cybercrime* yang mengganggu rasa keadilan tersebut dikaitkan dengan ketentuan pidana yang berlaku. KUHP tidak mampu mengkoordinir segala bentuk kejahatan yang sudah berkembang pesat. Hal ini karena KUHP merupakan produk lama sementara *cybercrime* merupakan dunia masa kini yang mengandalkan teknologi tinggi. Namun jika dikaji menggunakan pendekatan *interpretasi* atau penafsiran terhadap undang-undang, yakni dengan Penafsiran *ekstensif,* merupakan untuk memperluas pengertian dari suatu istilah yang berbeda dengan pengertiannya yang digunakan dalam istilah sehari-hari. Penerapan KUHP terhadap tindak pidana *hacking* maupun *cracking* substansinya hampir sama dengan rumusan tindak pidana biasa dalam KUHP, rumusan perbuatan yang dimaksud dalam *hacking* adalah sebuah aktivitas dimana untuk melakukan akses secara melawan hukum atau ilegal terhadap sistem komputer

dalam dunia internet. Sedangkan rumusan dalam KUHP adalah memasuki atau melintas batas wilayah secara tidak sah, hal ini seperti yang dimaksud dalam pasal 167 KUHP. Untuk itulah diperlukan perangkat hukum yang baru pula untuk mengimbangi perkembangan zaman yang tanpa sadar telah melampaui jangkauan ketentuan hukum yang ada. Hukum diyakini sebagai alat untuk memberikan kepastian penegakan hukum dalam pergaulan hidup.

Dalam upaya penegakan hukum dalam ruang *cyber (Cybercpace)* untuk para pelaku tindak pidana *hacking* dan *cracking* memang tidak dijelaskan secara rinci di dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Walaupun tidak diatur secara rinci pasal mengenai *hacking* dan *cracking* bukan berarti para pelaku tindak pidana dapat bebas, karena didalam pasal 30 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pada tindak pidana *hacking* dan *cracking* telah diatur dan dirumuskan dalam pasal-pasal yang dapat menjerat pelaku. Pada dasarnya tindak pidana *hacking* diatur secara umum pada pasal 30 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi sebagai berikut:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Menurut Sutan Remy didalam bukunya Kejahatan dan Tindak Pidana Komputer, yang diatur dalam pasal 30 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik terdiri atas:[137]

1) Membobol komputer dan/atau sistem elektronik yang bertujuan untuk mengakses saja tanpa tujuan;
2) Membobol komputer dan/atau komputer yang selain bertujuan untuk mengakses adalah juga untuk memperoleh informasi dan dokumen elektronik;
3) Membobol komputer dan/atau sistem elektronik yang bertujuan selain untuk mengakses juga untuk menaklukan sistem pengaman dari sistem komputer yang diakses itu.

Dari 3 (tiga) ayat dalam pasal 30 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur tentang tindak pidana *hacking*

[137] Sutan Remy Syahdeini, *Kejahatan dan Tindak Pidana Komputer*, Jakarta, Pustaka Utama Grafiti, 2008, halaman. 240

ini dapat dijelaskan bahwa unsur-unsur yang termuat dalam tindak pidana *hacking* tersebut:

b. Pasal 30 Ayat (1) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:[138]

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun".

Unsur-unsur tindak pidana dalam ayat (1) yaitu:

1. Unsur "setiap orang" :

Disini berarti setiap orang yang sebagai subjek hukum dapat bertanggungjawab dan cakap hukum sesuai diatur dalam perundang-undang serta badan hukum yang berbadan hukum sesuai ketentuan perundang-undangan.

2. Unsur "dengan sengaja dan tanpa hak atau melawan hukum" :

Disini berarti perbuatan yang dilakukan oleh seseorang itu dilakukan dengan sengaja dan penuh kesadaran bahwa perbuatan yang dilakukan melawan hukum.Dalam hal melawan hukum berarti ada suatu peraturan tertulis yang merumuskan dan menyatakan perbuatan tersebut dilarang oleh hukum secara positif tertulis dalam perundangundangan di Indonesia.

3. Unsur "mengakses Komputer dan/atau Sistem Elektronik milik Orang lain" :

Disini mengakses komputer dan/atau sistem elektronik milik orang lain dapat dijelaskan bahwa perbuatan mengakses disini adalah suatu kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam

[138] Pasal 30 Ayat (1) Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

jaringan, melalui seperangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengummkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Perlu diketahui pula bahwa objek dalam tindak pidana peretasan (hacking) ini adalah komputer dan/atau sistem elektronik yang merupakan wilayah ataupun daerah privasi seseorang yang dilindungi keberadaannya.

4. Unsur "dengan cara apapun" :

Bahwa terdapat berbagai macam cara yang dilakukan untuk dapat mengakses komputer dan/atau sistem elektronik milik orang lain. Apakah secara langsung dengan menggunakan perangkat keras milik korban ataukah dengan menggunakan jaringan internet.

Dalam pasal 30 ayat (1) ini murni bahwa seseorang dilarang mengakses komputer dan/atau sistem elektronik milik orang lain yang merupakan daerah privasi seseorang. Ruang privat adalah ruang yang bersifat pribadi dan hanya dapat dimasuki oleh orang- orang yang memiliki kode akses tertentu. Apabila dimasuki dan informasi yang ada didalamnya disebarluaskan, maka dalam hal tersebut akan menimbulkan kerugian yang tidak sedikit jumlahnya. Dapat dianalogikan dalam pasal 167 Kitab Undang-undang Hukum Pidana dimana seseorang dilarang masuk kerumah atau pekarangan orang lain tanpa seijin pemilik rumah. Seperti halnya pasal 30 ayat (1) ini bahwa komputer dan/atau sistem elektronik merupakan privasi orang yang dilindungi keberadaannya.

Perumusan *hacking* sebagai tindak pidana dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008

tentang Informasi dan Transaksi Elektronik pasal 30 ayat (1) diatas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana pasal 46 ayat (1) yaitu:

> Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1), dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

c. Pasal 30 Ayat (2) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Unsur-unsur tindak pidana dalam pasal 30 ayat (2) sama seperti pada ayat (1) namun dalam ayat (2) ini ditambahkan unsur "dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Disini dapat diterangkan bahwa seseorang dalam hal mengakses komputer dan/atau sistem elektronik orang lain tanpa hak dan dengan cara apapun dimaksudkan untuk suatu tujuan tertentu, yaitu memperoleh informasi elektronik dan/atau dokumen elektronik. Kejahatan ini dapat berupa pencurian data atau dokumen elektronik yang digunakan untuk tujuan terntentu.Misalnya dalam persaingan dagang seorang hacker dibayar oleh suatu perusahaan untuk mencuri informasi yang berkaitan dengan perusahaan saingannya dengan tujuan mencari keuntungan sebesar-besarnya. Dapat pula berupa memasuki sistem elektronik orang lain untuk mencari data-data tertentu semisal password *e-banking* seseorang. Yang kemudian

setelah mengetahui paswoord-nya, maka pelaku mencuri uang dengan membelanjakannya melalui internet.

Perumusan *hacking* sebagai tindak pidana dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 30 ayat (2) diatas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana pasal 46 ayat (2) yaitu:

> Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2), dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).

c. Pasal 30 Ayat (3) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

   > Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Unsur yang ditonjolkan dalam ayat (3) ini yaitu unsur “dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan”.Dalam unsur ini berarti bahwa *Hacker* yang melakukan kejahatannya dengan menerobos sistem keamanan atau dalam ilmu komputer disebut firewall. Para *hacker* menggunakan berbagai aplikasi *tools hacking* dalam melakukan kejahatannya.Dimana aplikasi tersebut berguna untuk menerobos atau menjebol sistem keamanan suatu sistem elektronik. Hal ini dapat dianalogikan dengan memasuki rumah orang lain tanpa ijin dengan menjebol engsel pintu/jendela yang ketentuan pidananya diatur dalam pasal 167 ayat (2) Kitab Undang-undang Hukum Pidana. Unsur “dengan

melanggar, menerobos, melampaui, atau menjebol sistem keamanan" menjadi menonjol dalam ayat ini karena memang cara-cara tersebut sering dipakai oleh *hacker* dapat melakukan kejahatannya.

Perumusan *hacking* sebagai tindak pidana dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 30 ayat (3) diatas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana pasal 46 ayat (3) yaitu:

> Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (3), dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

d. Pasal 32 Ayat (1) Undang-undang Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan bahwa :

   > 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.

Pada pasal 32 ini merupakan pasal dapat digunakan untuk menjerat *hacker* yang juga melakukan *cracking* memuat unsur subjektif yang dilakukan oleh yaitu pelaku, Dalam unsur ini berarti bahwa *cracker* yang dimaksud dalam pasal ini adalah orang yang melakukan kejahatan atau pelaku harus memenuhi unsur bahwa dalam melakukan kejahatan tersebut pelaku tersebut sengaja, tanpa hak atau ijin, dan melanggar hukum dalam melakukan perbuatan itu, sedangkan unsur objektifnya adalah melakukan perbuatan dengan cara apapun mengubah,

menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik publik. Pasal 32 ayat (2) memuat unsur objektif melakukan perbuatan memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak

Dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini terdapat aturan tambahan yang mengatur mengenai tindak pidana yang telah diatur dam pasal-pasal sebelumnya. Pasal-pasal ini menjadi aturan tambahan yang dapat dijadikan pasal penjerat bagi penegak hukum untuk menjerat para pelaku *cybercrime*, diantaranya :

a. Pasal 36 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan bahwa :

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34 yang mengakibatkan kerugian bagi orang lain

   Unsur-unsur dalam pasal 36 yaitu:

   1. setiap orang;
   2. dengan sengaja dan tanpa hak atau melawan hukum;
   3. melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai pasal 34;
   4. mengakibatkan kerugian bagi orang lain.

Pengertian setiap orang disini, selain ditafsirkan sebagai individu juga badan hukum yang berbadan hukum sesuai ketentuan perundang- undangan. Pengertian dengan sengaja dan tanpa hak, dapat ditafsirkan sebagai perbuatan yang bertentangan dengan undang- undang dan tindakan melalaikan ancaman hukuman. Adapun perbuatan yang dilarang oleh undang-undang adalah melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34 dan akibatnya kerugian bagi orang lain.

Tindak pidana yang dimaksud dengan Pasal 36 adalah tindak pidana materiil atau tindak pidana dengan perumusan materiil, yaitu tindak pidana yang baru dianggap terlaksana penuh dengan timbulnya akibat yang dilarang. Dengan demikian akibat dari perbuatan yang dilarang undang-undang sebagaimana dimaksud di atas, yang mengakibatkan kerugian bagi orang lain harus dibuktikan.

Pengaturan *hacking* sebagai tindak pidana dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 36 diatas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana pasal 51 ayat (2) yaitu:

> Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan penjara paling lama 12 (dua belas) tahun dan/atau dengan paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).

b. Pasal 37 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan bahwa:

> Setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagamana dimaksud dalam pasal 27 sampai dengan pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada diwilayah yurisdiksi Indonesia.

Berkaitan dengan ketentuan pidana dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa terdapat pemberatan penjatuhan sanksi pidana pokok jika perbuatan-perbuatan yang dilakukan memiliki sifat-sifat yang memberatkan apabila dengan tindak pidana *hacking* itu sendiri.Pemberatan tersebut berdasarkan objek tindak pidana dan subjek tindak pidana.

a. Berdasarkan Objek Tindak Pidana *Hacking*:

1. Pasal 52 ayat (2) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik :

   > Dalam hal perbuatan sebagaimana dimaksud dalam pasal 30 sampai pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.

   Berdasarkan hal tersebut di atas dapat diketahui bahwa pemberatan pidana ditambah sepertiga jika objek tindak pidananya berupa sistem elektronik milik pemerintah yang digunakan untuk layanan publik.Pemberatan ini didasarkan pada dampak kerugian yang ditimbulkan oleh cyber crime dalam hal ini berawal dari *hacking* dan *cracking* jika merusak situs atau web layanan publik milik pemerintah.

2. Pasal 52 ayat (3) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik :

> Dalam hal perbuatan sebagaimana dimaksud dalam pasal 30 sampai pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan, dan diancam dengan pidana pokok masing- masing pasal ditambah dua pertiga.

Berdasarkan hal diatas diketahui bahwa tindak pidana *cybercrime* baik itu *hacking* maupun *cracking* dimana perbuatan tersebut menyerang situs atau web pemerintah yang dianggap penting dan strategis maka pidana pokok ditambah duapertiga tiap Pasalnya.Hal ini mengindikasikan bahwa sistem elektronik badan strategis pemerintah sangat dilindungi dari tindakan *hacker*. Badan strategis tersebut berkaitan dengan keamanan negara dan stabilitas negara. Maka dari itu perlu pengamanan yang ketat baik dari segi hukum maupun segi sistem keamanannya.

b. Berdasarkan Subjek Tindak Pidana Peretasan (*Hacking*) :

Dalam Pasal 52 ayat (4) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatakan bahwa :

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

Berdasarkan pasal 52 ayat (4) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diketahui bahwa pemberatan sanksi pidana didasarkan pada pelaku tindak pidana yang merupakan suatu korporasi.Korporasi bisa dikatakan sebagai suatu lembaga atau badan ataupun organisasi yang memiliki struktur kepengurusan baik itu berupa suatu perusahaan ataupun badan

hukum lainnya. Ketentuan tersebut di atas dimaksudkan untuk menghukum setiap perbuatan yang memenuhi unsur sebagaimana dalam pasal 27 sampai dengan pasal 37 yang dilakukan oleh koorporasi (*corporate crime*) dan/atau staf yang memiliki kapasitas untuk:

1. mewakili korporasi;
2. mengambil keputusan dalam korporasi;
3. melakukan pengawasan dan pengendalian dalam korporasi;
4. melakukan kegiatan demi keuntungan korporasi.

Salah satu contoh penegakan hukum terhadap kejahatan *hacking* dan *cracking* dengan menggunakan tehnik *defacing* yang pernah di ungkap oleh aparat penegak hukum adalah kasus Peretasan Website Presiden Susilo Bambang Yudhoyono (SBY) yang terjadi pada 9 Januari 2013 yang dilakukan oleh terdakwa Wildan Yani Ashari alias yayan alias MJL007 (nama akun samaran). Dalam aksinya, Wildan melakukan deface atau mengganti tampilan asli halaman utama situs resmi Presiden SBY, Presidensby.info. Berawal ketika Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada hari dan tanggal yang sudah tidak dapat diingat di pertengahan tahun 2012 sampai dengan tanggal 08 Januari 2013 sekitar pukul 22:45 WIB atau setidak- tidaknya pada waktu lain dalam tahun 2012 sampai dengan bulan Januari 2013 bekerja di CV. Surya Infotama, yang beralamat di Jalan Letjen Suprapto Nomor 169, Kebon Sari Kab. Jember, Jawa Timur dimana selaku operator billing pada warung internet (warnet) Surya Com milik CV. Surya Infotama. Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 telah meretas server my.techscape.co.id dan membuat akun secara ilegal

pada webshosting www.jatirejanetwork.com dengan menggunakan seperangkat komputer billing milik warung internet (warnet) Surya Com milik CV. Surya Infotama dengan ip address-nya adalah 210.247.249.58 yang bergerak dibidang pelayanan *domain hosting*, dimana dimiliki dan dikelola oleh Saksi Eman Sulaiman bin Enje yang dibeli dari Saksi D.A. Giovanno Setyawardhana.[139]

Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan sebuah celah keamanan pada website www.jatirejanetwork.com kemudian melakukan *SQL Injection* dan berhasil menanamkan sebuah *backdoor* berupa *tools software* yang berbasis bahasa pemograman PHP bernama wso.php (*web sell by orb*) dan disimpan kedalam harddisk komputer billing warung internet (warnet) Surya Com tersebut pada drive D :Master pada folder : 001-MasterSoftware/009-Tool/Root. Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan keamanan server website yang sama dengan *ip address*-nya dengan techscape.co.id milik CV. Techscape dengan *ip address*-nya adalah 202.155.61.121 dan menemukan celah keamanan, sehingga dapat disimpulkan bahwa servertechscape.co.id memiliki celah keamanan yang sama, kemudian Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan *reserve ip lookup* terhadap website yang dimaksud dengan menggunakan *tool on line* (*web based*) www.yougetsignal.com yang dimana Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 berhasil mendapatkan infomasi bahwa website tersebut memiliki ip address-nya adalah 202.155.61.121, kemudian Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan dan menemukan

---

[139] Putusan Pengadilan Jember Nomor 253/Pid.B/2013/PN.JR, Direktori Putusan Mahkamah Agung, https://putusan.mahkamahagung.go.id/putusan/c2aca409d0ac7983a6329eb519433ac7, Akses tanggal 14 Agustus 2019

satu website yang merupakan sebuah jasa penyewaan *server* dan aplikasi atau software dimana untuk keperluan *web server* (*webhosting*) yaitu www.techscape.co.id kemudian Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mencari direktori yang didalamnya terdapat konfigurasi *web host manager complete solution* (WHMSC). WHMSC adalah sebuah aplikasi yang biasa digunakan untuk webhosting management dan Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 berhasil menemukan *direktori* yang dimaksud yaitu my.techscape.co.id.[140]

Sekitar bulan November 2012, Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 telah berhasil menerobos website www.jatirejanetwork.com dengan menggunakan teknik *SQL Injection* dan Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 telah menanamkan backdoor wso untuk menjalankan *command linux* : cat/home/tech/www/my/configuration/php, melalui *backdoor* wso yang telah ditanam sebelumnya Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 telah berhasil mendapatkan *username* dan *password* dari *database* WHMCS yang dikelola oleh pihak techscape dengan username : "tech_whmcs" dan password : "yl6=V=!J&mL", yang kemudian Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menjalankan tool WHMKiller dari domain website www.jatirejanetwork.com.[141]

Dari website www.jatirejanetwork.com, Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 bisa mendapatkan username dan password dari domain manager pada setiap *domain name* yang ada di *serverwebhosting* dari WHM

[140] *Ibid.,*
[141] *Ibid.,*

control panel dimana *username*-nya adalah *"root"* dan *password*-nya adalah "b4p4kg4nt3ngTIGA" dengan nomor port : 2086, kemudian Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses ke techscape.co.id dengan *ip address*-nya adalah 202.151.61.121 dengan nomor port 2086 melalui *browser Mozilla Firefox*. Setelah mendapatkan akses ke *WHM Control Panel*, Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melalukan *log in* dengan mengisi *username "root'*dan *password* "b4p4kg4nt3ngTIGA" kemudian Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menanamkan sebuah *tool backdoor* wso.php pada servertechscape.co.id dengan cara *uploading tool backdoor* wso.php pada servertechscape.co.id pada tanggal 16 November 2012, jam 04:58:31 WIB.[142]

Agar *backdoor* tersebut tidak diketahui oleh admintechscape.co.id maka Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perubahan nama (rename) terhadap *tool* yang dimaksud menjadi "domain.php" yang mana ditempatkan di sub direktori my.techscape.co.id/feeds/, sehingga Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dapat mengakses *server* techscape.co.id kapanpun melalui url "my.techscape.co.id/feeds/domain.php" dengan password "yayan123". Pada tanggal 08 Januari 2013, sekitar jam 20:00 WIB, Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mengakses ke website www.enom.com selaku domain register untuk techscape.co.id, kemudian Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan log in ke akun techscape dengan username-nya adalah "techscape" dan password-nya

[142] *Ibid.,*

adalah “tsc800puri”. Setelah berhasil melakukan log in ke akun techscape di domain register enom (eNom, Inc, USA), dari situlah Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mendapatkan informasi tentang DNS Server dari domainpresidensby.info , diantaranya adalah :

1) sahi78679.earth.orderbox-dns.com;
2) sahi78679.mars.orderbox-dns.com;
3) sahi78679.venus.orderbox-dns.com;
4) sahi78679.mercury.orderbox-dns.com.

kemudian, Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 merubah DNS Server menjadi :

1) id1.jatirejanetwork.com; dan
2) id2.jatirejanetwork.com. [143]

Kemudian, Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada jam 22:45 WIB membuat (*create*) akun *domainpresidensby.info* di server perusahaan webhosting yaitu jatirejahost.com dan menempatkan sebuah file HTML “Jember HackerTeam” di serverjatirejahost.cdikdiksiom, sehingga ketika para user internet akan mengakses konten websitewww.presidensby.info yang sebenarnya, justru website yang akan terakses adalah tampilan file HTML “Jember Hacker Team”.

Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 berhasil meretas server my.techscape.co.id milik CV.Techscape dan membuat account secara ilegal pada webhosting di websitewww.jatirejanetwork.com milik dan dikelola oleh

[143] *ibid.,*

Saksi Eman Sulaiman bin Enjen, dimana dengan menggunakan tools khusus berupa script khusus yang berbasis bahasa pemrograman PHP dengan modus redirecting DNS sehingga Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dapat berinteraksi dengan sistem milik my.techscape.co.id dan www.jatirejanetwork.com yang mana keduanya merupakan penyedia webhosting dan bertindak sebagai Internet Service Provider (ISP) yang merupakan penyelenggara multimedia yang termasuk bagian dari Penyelenggara Jasa Telekomunikasi dan Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan hal tersebut tanpa seijin dari CV.Techscape dan Saksi Eman Sulaiman bin Enjen.[144]

Dalam putusan Pengadilan Negeri Jember Nomor 253/Pid.B/2013/PN.JR, terdakwa Wildan Yani Ashari alias Yayan alias MJL007 terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana dengan sengaja dan tanpa hak melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, sesuai dengan isi Pasal 30 Ayat 1 Undang-undang Nomor 11. Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Terdakwa diganjar dengan sanksi hukum berupa pidana penjara 6 (enam) bulan dan denda sebesar Rp.250.000,- (dua ratus lima puluh ribu rupiah) subsidair 15 (lima belas) hari kurungan.

Melihat kenyataan kasus tersebut diatas, Dalam menegakan hukum pidana atas pertanggung jawaban pidana atas perbuatannya, Menurut Eddy O.S. Hiariej seseorang harus memenuhi 3 (tiga) syarat yaitu:

---

[144] *ibid.,*

1) Kemampuan bertanggungjawab;
2) Hubungan psikis pelaku dengan perbuatan yang dilakukan;
3) Tidak ada alasan yang penghapus pertanggungjawaban pidana berupa alasan pembenar yang menghapuskan sifat melawan hukumnya perbuatan dan alasan pemaaf yang menghapuskan sifat dapat dicelanya pelaku.[145]

Apabila ditinjau dari aspek pertama pertanggung jawaban pidana, yakni kemampuan bertanggungjawab, terdakwa sudah memenuhi kriteria untuk dapat bertanggungjawab. Hal ini didasari pada fakta-fakta sebagai berikut:

a. Terdakwa sebagai subjek hukum, yang memiliki hak dan kewajiban dimata hukum, telah cakap hukum. Dimana pada saat para terdakwa melakukan perbuatannya, terdakwa sudah berumur lebih dari 18 tahun dan sudah dianggap dewasa dan mampu bertanggungjawab secara hukum;
b. Terdakwa tidak mengalami kekurangsempurnaan akal atau sakit ingatan, sehingga ketentuan pasal 44 ayat (1) KUHP tidak berlaku bagi para terdakwa;
c. Terdakwa dapat mengetahui ketercelaan dari tindakan yang dilakukannya, yakni dengan melakukan penganiayaan terhadap anak yang mengakibatkan kematian;
d. Terdakwa memiliki kemampuan jiwa untuk dapat menentukan kehendaknya atas tindakan tersebut, apakah dilaksanakan atau tidak, namun terdakwa lebih memilih untuk melakukan tindak pidana tersebut;
e. Terdakwa menegetahui perbuatan yang dilakukannya itu dapat dicela di dalam masyarakat.

---

[145] Eddy O.S. Hiariej, *Prinsip-Prinsip Hukum Pidana*, (Yogyakarta: Cahaya Atma Pustaka, 2014), hlm 93.

Dalam mempertimbangkan unsur-unsur pada dakwaan pertama yakni pasal 46 ayat (1) jo. pasal 30 ayat (1) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dengan penjabarannya sebagai berikut:

1) Barangsiapa

Bahwa pada unsur pertama yang dimaksud dengan kata barang siapa menurut doktrin Hukum Pidana adalah setiap orang yaitu siapa saja yang ditujukan kepada manusia sebagai subjek atau siapa saja sebagai pelaku tindak pidana dan perbuatan itu dapat dipertanggungjawaban kepadanya serta tidak terdapat ha-hal yang dapat menghapus kesalahannya. Dalam perkara ini menurut Putusan Nomor 253/PID.B/2013/PN.JR, terdakwa atas nama Wildan Yani Ashari alias Yayan alias MJL007 merupakan pelaku peretasan *hacking* dan *cracking* . Terdakwa membenarkan identitas yang tercantum dalam dakwaan, sehat secara jasmani dan rohani sehingga mampu dimintakan pertanggungjawabannnya. Terdakwa juga berdasarkan fakta-fakta hukum yang ditemukan Majelis Hakim, membenarkan setiap keterangan saksi dan juga tidak terdapat alasan pembenar dan pemaaf sebagai alasan penghapus pidana. Dalam hal ini, unsur "barangsiapa" telah terpenuhi.

2) Dengan Sengaja dan Tanpa Hak atau Melawan Hukum Mengakses Komputer dan/atau Sistem Elektronik Milik Orang Lain Dengan Cara Apapun

Bahwa pada unsur kedua ini, yang dimaksud dengan sengaja adalah perbuatan yang dilakukan oleh seseorang itu dilakukan dengan sengaja dan penuh kesadaran bahwa perbuatan yang dilakukan melawan hukum.Begitu juga dalam

hal unsur melawan hukum berarti ada suatu peraturan tertulis yang merumuskan dan menyatakan perbuatan tersebut dilarang oleh hukum secara positif yang tertulis dalam perundang-undangan di Indonesia.Pada makna mengakses mempunyai pengertian yakni sebuah kegiatan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan.

Demikian pula dengan makna komputer adalah sebuah alat untuk memproses data elektronik, magnetic, optic, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.Sedangkan, sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Setelah Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sadar betul sudah meretas websitewww.presidensby.infodan Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 tidak langsung mengembalikan kembali tampilan website tersebut seperti semula, maka tindakan pengalihan tampilan tersebut merupakan perbuatan yang disengaja dan diinsyafi oleh Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dikarenakan Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 lupa untuk mengembalikan tampilan website tersebut seperti semula. Dalam hal ini, unsur “dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun” telah terbukti secara sah dan meyakinkan menurut hukum.

Berdasarkan rendahnya sanksi yang diberikan apabila melihat di dalam amar putusan hakim yang menjatuhkan pidana penjara selama 6 (enam) bulan terhadap terdakwa dikurangi masa penahanan jika dibandingkan dengan surat Tuntutan Jaksa Penuntut Umum yakni menuntut dengan menjatuhkan pidana penjara selama 10 bulan dikurangi selama terdakwa berada dalam tahanan, apabila mengkaji di dalam pasal 46 ayat (1) jo pasal 30 ayat (1) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dengan perbuatan yang dihukum karena melakukan peretasan (hacking) adalah hukuman penjara selama-lamanya 6 (enam) tahun dan denda paling banyak sebesar Rp. 1.000.000.000,- (satu miliar rupiah), maka sangatlah beralasan hukum dinilai akan mempersulit untuk mencapai tujuan nilai keadilan daripada pemidanaan itu sendiri, karena dengan sanksi yang dijatuhkan terlalu kecil sehingga tidak dapat memberikan efek jera terhadap terdakwa sehingga nantinya dikhawatirkan terdakwa akan kembali melakukan tindak pidana *hacking* dan *cracking*.

Dasar pertimbangan Hakim dalam menjatuhkan putusan dalam penagakan hukum pidana terhadap tindak pidana *hacking* dan *cracking* ini didasarkan pada banyak hal. Diantaranya adalah bukti- bukti yang diajukan, keterangan saksi, keterangan terdakwa, dan surat dakwaan yang diajukan oleh Jaksa Penuntut Umum. Putusan yang dijatuhkan kepada terdakwa dalam kasus peretasan *(hacking)* pun pada dasarnya termasuk dalam teori pemidanaan relatif, yaitu penjatuhan hukuman harus memiliki tujuan tertentu, bukan hanya sekadar sebagai pembalasan.Tujuan pemidanaan tersebut dapat sebagai pencegahan terhadap tindak pidana *hacking* dan *cracking* khususnya bagi masyarakat.Oleh karena itu,

hendaknya peraturan perundang-undangan di Indonesia dalam pengaturan mengenai peretasan (hacking) lebih diatur secara khusus dan efektif.

B. Aspek Pembuktian Terhadap Tindak Pidana *Hacking* Dan *Cracking*

Pembuktian dalam hukum pidana merupakan sub sistem kebijakan kriminal sebagai *science of response* yang mencakup berbagai disiplin ilmu. Hal ini disebabkan oleh luasnya kausa dan motif berkembangnya jenis kejahatan yang berbasis teknologi informrmasi saat ini. Pada hakekatnya, pembuktian dimulai sejak adanya suatu peristiwa hukum. Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan (serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyelidikan menurut cara yang diatur dalam undang-undang ini), yang diatur dalam Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian dalam pasal 1 angka 13.

Menurut M.Yahya Harahap, pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa.[146] Menurut Pitlo, "pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya".[147] Menurut Subekti, yang

---

[146] M.Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*,Op.Cit., Halaman 73

[147] Edmon Makarim, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, 2003,halaman. 417.

dimaksudkan dengan "membuktikan" adalah meyakinkan hakim tentang kebenaran dalil ataupun dalil-dalil yang dikemukakan oleh para pihak dalam suatu persengketaan."Pembuktian tentang benar tidaknya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting dalam hukum acara pidana".[148]

Berhadapan dengan kasus *cybercrime*, pembuktian menjadi masalah yang pelik. Seringkali penegak hukum di Indonesia mengalami kesulitan saat menjerat pelaku *cybercrime* karena masalah pembuktian (*documentary evidence*) yang tidak memenuhi ketentuan sistem hukum pidana Indonesia. Sementara upaya penjeratan terhadap pelaku-pelaku *cybercrime* harus tetap dilakukan, upaya perluasan menjadi solusi untuk menegakan hukum.

Hukum pembuktian merupakan sebagian dari hukum pidana yang mengatur tentang alat-alat bukti yang sah menurut hukum, barang-barang bukti, sistem pembuktian yang dianut, syarat dan tata cara pembuktian yang dilakukan, serta kewenangan hakim untuk menerima, menolak dan menilai suatu pembuktian. Sumber hukum pembuktian adalah undang-undang, doktrin dan yurisprudensi. Oleh karena itu, Undang-undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana (KUHAP) menjadi salah satu sumber hukum dalam proses pembuktian.

Pembuktian merupakan titik sentral pemeriksaan perkara dalam sidang pengadilan. Pembuktian adalah ketentuan- ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang untuk membuktikan

[148] Subekti, *Hukum Pembuktian, Pradnya Paramita*, Jakarta, 1995, hal. 1.

kesalahan yang didakwakan kepada terdakwa. Pembuktian juga merupakan ketentuan yang mengatur alat- alat bukti yang dibenarkan undang-undang yang dapat dipergunakan hakim dalam membuktikan kesalahan terdakwa. Oleh karena itu, hakim tidak dapat mempergunakan alat bukti yang bertentangan dengan undang-undang. Kebenaran atas suatu putusan harus teruji dengan alat bukti yang sah secara hukum serta memiliki kekuatan pembuktian yang melekat pada setiap alat bukti yang ditemukan.

Berdasarkan Undang- Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, maka yang dinilai sebagai alat bukti dan yang dibenarkan mempunyai "kekuatan pembuktian" hanya terbatas kepada alat bukti yang tercantum dalam Pasal 184 ayat (1) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana. Dengan kata lain, sifat dari alat bukti menurut Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana adalah limitatif atau terbatas pada yang ditentukan saja, sehingga apabila ada barang bukti yang tidak termasuk dalam klasifikasi alat bukti menurut pasal 184 ayat (1) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana maka barang bukti tersebut tidak sah menurut Undang-undang tersebut. Seiring berkembangnya teknologi Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana mengenai alat bukti sudah tidak dapat lagi mengikut pesatnya perkembangan jaman. Oleh karena itu, diundangkannya Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Didalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik terdapat perluasan dari pengertian alat bukti (limitatif) yang terdapat di Undang-undang Nomor 8 tahun 1981 tentang Hukum Acara Pidana. Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah ketentuan yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.[149] Pasal 1 angka 1 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan definisi mengenai apa yang dimaksud dengan Informasi Elektronik, yaitu:

> satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, angka, Kode Akses, symbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Lebih lanjut, Pasal 5 ayat (2) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menegaskan bahwa:

> Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya... merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

---

[149] Yanto awaludin, *Undang-undang Informasi Dan Transaksi Elektronik,* http://selalucintaindonesia.wordpress.com/2013/01/15/undang-undang-informasi-dan-transaksi-elektronik/, akses 17 Agustus 2019

Ketentuan ini menegaskan bahwa alat bukti elektronik telah diterima dalam sistem hukum pembuktian di Indonesia di berbagai peradilan, seperti peradilan pidana, perdata, agama, militer, tata usaha negara, mahkamah konstitusi, termasuk arbitrase.[150]

Pemahaman "perluasan" tersebut haruslah dihubungkan dengan Pasal 5 ayat (1) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Perluasan yang dimaksud ialah sebagai berikut:

a) Memperluas jumlah alat bukti yang diatur dalam Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana. Dalam Undang- Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana diatur 5 (lima) alat bukti. Berdasarkan Pasal 5 Undang-undang Nomor 11 Tahun 2008 maka alat bukti dalam Undang-undang No 8 Tahun 1981 tentang Hukum Acara Pidana ditambah satu alat bukti yaitu Alat Bukti digital/elektronik.
b) Memperluas cakupan alat bukti yang diatur dalam Undang-undang No 8 Tahun 1981 tentang Hukum Acara Pidana. Hasil cetak dari Informasi digital atau Dokumen Elektronik secara hakiki ialah surat. Alat bukti surat telah diatur dalam Undang-undang No 8 Tahun 1981 tentang Hukum Acara Pidana.

[150] Josual Sitompul, *Legalitas Hasil Cetak Tweet Sebagai Alat Bukti Penghinaan*, http://www.hukumonline.com/klinik/detail/lt502a53fad18dd/legalitas-hasil-cetak-tweet- sebagai-alat-bukti-penghinaan, diakses pada tanggal 17 Agustus 2019

c) Perluasan juga dimaksudkan bahwa Informasi Elektronik atau Dokumen Elektronik dapat dijadikan sumber petunjuk sebagaimana dimungkinkan dalam beberapa Undang-undang.[151]

Namun tidak sembarang informasi elektronik atau dokumen elektronik dapat dijadikan alat bukti digital yang sah. Menurut Pasal 6 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, suatu informasi elektronik atau dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu sistem elektronik yang andal dan aman, serta memenuhi persyaratan minimum sebagai berikut:[152]

a. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;
b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;

[151] http://warungcyber.web.id/?p=84 diakses pada tanggal 17 Agustus 2019
[152] H.P. Panggabean, *Hukum Pembuktian Teori-Praktik dan Yurisprudensi Indonesia, Alumni*, Bandung, 2014, halaman 281

d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan
e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk

Pihak yang mengajukan Alat bukti digital tersebut harus dapat membuktikan bahwa telah dilakukan upaya yang patut untuk memastikan bahwa suatu sistem elektronik telah dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik tersebut. Dari Pasal 1 Angka 4, Pasal 5 Ayat (3), Pasal 6 dan Pasal 7 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat dikategorikan syarat formil dan materiil dari dokumen elektronik agar mempunyai nilai pembuktian, yaitu:[153]

1) berupa informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan, yang dapat dilihat, ditampilkan dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tulisan, suara, gambar...dan seterusnya yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya;
2) dinyatakan sah apabila menggunakan/berasal dari Sistem Elektronik sesuai dengan ketentuan yang diatur dalam undang-undang;

[153] *Ibid.,*

3) dianggap sah apabila informasi yang tecantum didalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Uraian mengenai syarat-syarat formil dan materiil tersebut menjelaskan bahwa dokumen elektronik agar memenuhi batas minimal pembuktian haruslah didukung dengan saksi ahli yang mengerti dan dapat menjamin bahwa sistem elektronik yang digunakan untuk membuat, meneruskan, mengirimkan, menerima atau menyimpan dokumen elektronik adalah sesuai dengan ketentuan dalam undang-undang; kemudian juga harus dapat menjamin bahwa dokumen elektronik tersebut tetap dalam keadaan seperti pada waktu dibuat tanpa ada perubahan apapun ketika diterima oleh pihak yang lain (*integrity*), bahwa memang benar dokumen tersebut berasal dari orang yang membuatnya (*authenticity*) dan dijamin tidak dapat diingkari oleh pembuatnya.[154] Hal ini bila dibandingkan dengan bukti tulisan, maka dapat dikatakan dokumen elektronik mempunyai derajat kualitas pembuktian seperti bukti permulaan tulisan (*begin van schriftelijke bewijs*), dikatakan seperti demikian oleh karena dokumen elektronik tidak dapat berdiri sendiri dalam mencukupi batas minimal pembuktian, oleh karena itu harus dibantu dengan salah satu alat bukti yang lain. Nilai kekuatan pembuktiannya diserahkan kepada pertimbangan hakim, yang dengan demikian sifat kekuatan pembuktiannya adalah bebas.

Dalam kejahatan *hacking* dan *cracking* Bukti Digital/elektronik dalam kejahatan *hacking* dan *cracking* yang bisa ditemukan adalah berupa *data log* yang

[154] *Ibid.,*

tersimpan dalam server suatu jaringan *internet service protocol* (ISP), dimana data informasi elekronik berupa dokumen elektronik yang tersimpan dalam memori *(log.)* tersebut merupakan jejak rekaman aktivitas penggunaan internet. Rangkaian tersebut berupa *algoritma-algoritma* yang memiliki arti khusus. hasil cetak *log* yang dapat dijadikan alat bukti yang sah sesuai dengan pasal 5 ayat 1 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian dapat diambil bukti petunjuk berdasarkan keterangan terdakwa.

Sebagai contoh pada putusan Pengadilan Negeri Jember Nomor 253/Pid.B/2013/PN.JR kasus *hacking* dan *cracking* Website Presiden Susilo Bambang Yudhoyono (SBY) , beberapa alat bukti yang dijadikan dasar pertimbangan hakim dalam penjatuhan putusan sebagai berikut:[155]

1) Keterangan saksi, yaitu saksi dari penyidik mengenai adanya tindak pidana akses ilegal terhadap komputer yang dilakukan oleh Wildan Yani Ashari alias yayan alias MJL007;
2) Barang bukti berupa:
    a) 1 (satu) unit CPU warna merah merek Power Up dengan 1 (satu) buah internal harddisk merek Maxtor s/n: 9QZB887G kapasitas 80 GB;
    b) 1 (satu) unit CPU warna hitam merah merek Simbadda dengan 1 (satu) buah internal harddisk merek Seagater s/n: 5VP6GX7R kapasitas 1 TB;
    c) 1 (satu) keeping CD merek IZUMI Kapasitas 700 MB s/n: CD- R IZ-1; dan

[155] Putusan Pengadilan Jember Nomor 253/Pid.B/2013/PN.JR, *Op. cit*

d) 1 (satu) keeping DVD Primary Image warna putih kapasitas 4,76 GB s/n: 2117E22230913821.

3) Dokumen digital/elektronik berupa *log file database* perusahaan hosting techscape.co.id dalam format file notepad (.txt);

4) Pemeriksaan digital forensik pada barang bukti menunjukkan adanya data-data log yang dilalui pelaku dan membuktikan adanya *ilegal DNS redirection* pada situs presiden SBY; dan

5) Pada saat penangkapan pelaku mengakui bahwa MJL007 adalah dirinya dan juga yang melakukan *ilegal DNS redirection* pada situs presiden SBY.

Pembuktian kasus pada putusan nomor 253/Pid/B/2013/PN JR oleh penyidik jika diklasifikasikan ke dalam bukti Digital yang mencakup:

a. *Real evidence*, yaitu hasil rekamanan langsung dari suatu aktifitas elektronik, hasil penghitungan atau analisa oleh suatu sistem komputer yang telah bekerja sesuai dengan prosedur perangkat lunak yang digunakan untuk pemrosesan data atau informasi, rekaman data log dari sebuah server dalam internet, atau juga dapat berbentuk salinan (receipt) dari suatu peralatan seperti hasil rekaman kamera yang menggunakan sensor. Real evidence ini meliputi file database perusahaan hosting techscape.co.id dalam format file notepad (.txt) dan pemeriksaan digital forensik pada barang bukti menunjukkan adanya data-data log yang dilalui pelaku dan membuktikan adanya ilegal DNS redirection pada situs presiden SBY.

b. *Hearsay evidence*, yaitu dokumen atau rekaman yang merupakan hasil dari pemrosesan dengan menggunakan komputer yang kesemuanya adalah salinan atas sebuah informasi di atas kertas. Hearsay evidence meliputi BAP sanksi, BAP saksi ahli, BAP terdakwa, dan BAP barang bukti, serta barang bukti CD yang berisi file domain.php pada servertechscape dan DVD yang berisi file akses IP Address 180.247.245.185 pada server alvindevelopment.com
c. *Derived evidence*, yaitu kombinasi antara real evidence dan hearsay evidence. Penggunaan data atau pesan elektronik sebagai barang bukti di pengadilan dicari ada tidaknya suatu hubungan antara keduanya. Derive evidence meliputi komputer yang digunakan untuk melakukan tindak pidana dan ahli TI.

Dari uraian alat bukti di atas, pembuktian atas putusan Nomor 253/Pid B/2013/PN JR tentang *hacking* dan *cracking* Website Presiden Susilo Bambang Yudhoyono (SBY) terkait adalah pembuktian tindak pidana tersebut sudah sesuai dengan ketentuan hukum pembuktian pada KUHAP dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, karena memenuhi unsur objektif dan unsur subjektif dari tindak pidana akses ilegal terhadap sistem komputer.

BAB V
PENUTUP

A. Kesimpulan

Seiring Perkembangan teknologi informasi, salah satunya dengan adanya internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Namun dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi negatif. Yakni timbulnya berbagai kejahatan dunia maya *(cybercrime).* Diantara berbagai kejahatan *cybercrime* adalah akses sistem komputer secara ilegal *(hacking)* dan menimbulkan kerusakan *(cracking).*

Berdasarkan uraian-uraian yang dicantumkan pada bab-bab sebelumnya dapat diambil beberapa kesimpulan yang menjawab permasalahan dalam tesis ini, adapun kesimpulan tersebut :

1. Akses ilegal terhadap sistem komputer, baik *hacking* maupun *cracking* yang merupakan suatu bentuk tindak pidana kejahatan dunia maya *(cybercrime)*, dalam upaya penegakan hukumnya, meskipun dalam KUHP tidak menyebutkan secara *eksplisit* mengenai kejahatan *hacking* dan *cracking,* namun apabila dilihat dari Penafsiran *ekstensif* perbuatan tersebut dapat dipidana jika memenuhi unsur delik yang tercantum dalam pasal 167 dan 406 ayat (1) KUHP. Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik terdapat pengaturan Tindak Pidana

Hacking dan *cracking* Pengaturan tindak pidana *Hacking* dirumuskan pada Pasal 30 ayat (1), (2) serta (3) dan *cracking* Pasal 32 ayat (1) dan (3). bahwa pada dasarnya tindak pidana *hacking* maupun *cracking* merupakan suatu tindakan setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik orang lain dengan tujuan memperoleh informasi dan/atau dokumen elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Dimana *hacking* dapat merupakan sebuah tindakan awal bagi pelaku *cybercrime* untuk melakukan kejahatan lainnya dalam ruang *cyber*.

2. Dalam aspek pembuktian terhadap kejahatan *hacking* dan *cracking* menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah terjadi perluasan alat bukti sebagaimana yang sebelumnya telah diatur dalam Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana. Dalam Undang-undang Nomor 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana (KUHAP) diatur 5 (lima) alat bukti yakni Keterangan Saksi, Keterangan Ahli, Surat, Petunjuk dan Keterangan Terdakwa. Berdasarkan Pasal 5 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik maka alat bukti dalam Undang-undang No 8 Tahun 1981 tentang Hukum Acara Pidana ditambah satu alat bukti yaitu Informasi Elektronik dan Dokumen Elektronik. Inilah yang disebut dengan Alat Bukti Elektronik/alat bukti digital. Dalam kejahatan *hacking* dan *cracking*

kedudukan alat bukti digital mempunyai kedudukan yang khusus, karena sebagai satu-satunya bukti suatu aktivitas dengan menggunakan komputer yang kemudian ditambah dengan kerangan ahli sehingga memiliki kekuatan hukumdi depan sidang pengadilan. Sebagai syarat mutlak untuk dapat diterimanya alat bukkti digital didepan sidang pengadilan, suatu sistem harus dapat dipercaya kabsahannya *(trustworthy)* atau sesuai dengan ketentuan dalam undang-undang; kemudian juga harus dapat menjamin bahwa dokumen elektronik tersebut tetap dalam keadaan seperti pada waktu dibuat tanpa ada perubahan apapun ketika diterima oleh pihak yang lain (*integrity*), bahwa memang benar dokumen tersebut berasal dari orang yang membuatnya (*authenticity*) dan dijamin tidak dapat diingkari oleh pembuatnya.

B. Saran

Berdasarkan hasil kesimpualan tersebut, maka rekomendasi penelitian ini adalah sebagai berikut:

1. Mengingat dampak yang ditimbulkan tindak pidana *hacking* dan *cracking* sangat berbahaya bagi *privasi* seseorang maupun instansi atau lembaga hukum maka hendaknya pemilik situs atau website memberikan pengaman *software* komputer baik berupa penggunaan *firewall*, mengunci data dengan *password* yang tidak mudah *di enkripsi*, *mem-backup* data secara rutin dan berkala, dan berbagai macam pengamanan lainnya.
2. Pemerintah perlu mengeluarkan aturan main *hacking* dan *cracking* dengan mengeluarkan peraturan pemerintah selain untuk menjelaskan beberapa pasal yang masih mengambang (salah perspektif), selain itu agar tindak pidana

hacking dapat diatur secara lebih rinci dan memperjelas tindakan-tindakan apa saja yang di kemudian hari dapat berpotensi sebagai tindak pidana *hacking* maupun *cracking*. juga untuk memudahkan bagi profesional yang bergerak dalam bidang teknologi informasi, serta memberikan pendidikan kepada masyarakat melalui peraturan yang ada. Sehingga aktivitas mereka tetap terlindungi hukum.

3. Para penegak hukum sebaiknya lebih meningkatkan kualitas aparaturnya dalam bidang teknologi informasi. Hal ini diperlukan karena pelaku tindak pidana *hacking* maupun *cracking* adalah orang-orang yang memiliki tingkat kecerdasan yang tinggi dalam bidang teknologi informasi. Apabila hal ini telah terpenuhi maka tindak pidana ini tidak akan menjadi tindak pidana yang tergolong susah untuk ditanggulangi seperti yang dirasakan oleh masyarakat saat ini.

C. Penutup

Atas rahmat Tuhan yang kuasa, akhirnya penulis bisa menyelesaikan penelitian Tesis ini dengan segala daya upaya dan kekurangan yang ada dalam diri penulis. Dimana hal tersebut merupakan keinginan penulis untuk meneliti bidang yang menjadi interest penulis. Semoga tulisan ini dapat bermanfaat bagi dunia kelimuan di perguruan tinggi khususnya dan di Indonesia pada umumnya.

Penulis juga menyadari sepenuhnya, bahwa tidak ada yang sempurna dalam dunia ini, kesempurnaan hanyalah milik Allah. Jika dalam penelitian ini pembaca menemukan banyak kesalahan, kekurangan itu tidak lain karena

keterbatasan (dalam segala hal: ilmu, waktu, dana dan lain-lain) yang dimiliki penulis serta kurangnya kemampuan penulis dalam menguraikan kata-kata.

Akhirnya saran dan kritik dari pembaca dibutuhkan dalam penelitian ini, demi perbaikan dan penyempurnaan dari tulisan ini. Akhir kata, semoga tulisan ini berguna bagis semua pihak yang membacanya, serta menambah wacana pemikiran bagi kita semua. Amien.

DAFTAR PUSTAKA

Abdulkhadir Muhammad, *Hukum Dan Penelitian Hukum*, Citra Aditia Bakti, Bandung, 2004.

Andi Hamzah, *Hukum Acara Pidana Indonesia*, Jakarta, Sinar Grafika, 2005.

Aroma Elmina Martha, Perempuan Dan Kekerasan Dalam Rumah Tangga Di Indonesia Dan Malaysia, Yogyakarta:FH.UI1 PRESS, 2012.

Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: PT Raja Grafindo Persada, 2007.

Barda Nawawi Arief, *Upaya Non Penal dalam Kebijakan Penanggulangan Kejahatan*, makalah disampaikan pada seminar Kriminologi VI, Semarang, tanggal 16-18 September 1991.

Benard L. Tanya, *Teori Hukum Strategi Tertib Mannusia Lintas Ruang dan Generasi*, Yogyakarta: Genta Publishing , 2010.

Budi Raharjo, Keamanan Sistem Informasi Berbasis Internet, PT Insan Indonesia, Bandung, 1998-2005.

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

Computer Network Research Group, *Mengejar Hacker itu Mudah*, Bandung, 20 Mei 2004

Departemen Pendidikan Nasional, 2012, *Kamus Besar Bahasa Indonesia*, Pusat Bahasa (Edisi Keempat), PT. Gramedia Pustaka Utama, Jakarta.

Didik M. Arief Mansur, Cyber Law Aspek Hukum Teknologi Informasi, Bandung: Aditama ,2009.

Edmon Makarim, Kompilasi Hukum Telematika, Jakarta, Rajagrafindo Persada, 2003.

Friedman, *Teori dan Filsafat Hukum* , Jakarta : Rajawali Press, 1990.

H.P. Panggabean, *Hukum Pembuktian Teori-Praktik dan Yurisprudensi Indonesia*, Alumni, Bandung, 2014.

http://cuplis.net/2009/03/metode-penelitian-metris/ diakses tanggal, 2009

http://dictionary.cambridge.org,

http://id.wikipedia.org/wiki/Kejahatan_dunia_maya

http://www.bartleby.com,

https://www.cnnindonesia.com/teknologi/20190426125843-192-389855/bssn-23245-juta-serangan-siber-serbu-indonesia-di-2018.

Jan Ramelink, *Hukum Pidana,* Jakarta: Gramedia Pustaka Utama, 2003.

Jimly Asshiddiqie dan M.Ali Safa'at, Dari Hans Kelsen Tentang Hukum, Sekretariat Jenderal dan Kepaniteraan Mahkamah Konstitusi RI, Jakarta, 2006.

Jonathan, Sarwono. Metode Penelitian Kuantitatif dan Kualitatif, Graha Ilmu, Yogyakarta, 2006.

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

Lawrence M. Friedman, *Hukum Amerika, Sebuah Pengantar, Terjemahan dari Wishnu Basuki*, Jakarta : Tatanusa, 2001.

Lili Rasjidi, *Dasar-Dasar Filsafat Hukum*, Bandung : Citra Aditya Bakti, 1996.

Mardjono Reksodiputro, *Kejahatan komputer (Suatu catatan sementara dalam rangka KUHP Nasional yang akan datang) , dalam Kemajuan Pembangunan Ekonomi dan Kejahatan*, Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum UI, 1997.

Moelyatno, *Asas-asas Hukum Pidana*, Rineka Cipta, Jakarta , 2000, halaman 1.

Peter Mahmud Marzuki, *Penelitian Hukum*, Cet. Ke-6, Jakarta: Kencana, 2010.

Phillippe Nonet & Phillip Selznick, *Law and Society in Transition: Toward Tanggapanive Law,* London : Harper and Row Publisher, 1978.

Putusan Pengadilan Jember Nomor 253/Pid.B/2013/PN.JR

Roscoe Pound, *Contemporary Jurisdic Theory ,* dalam D Llyod (ed), *Introduction to Jurisprudence* ,London, Stences,1965.

Roscou Pound, *Pengantar Filsafat Hukum*, Jakarta : Bhratara Karya Aksara, 1982.

Ruslan, Rosdy. Metode Penelitian Publik. PT Raja Grafindo Persada, Surabaya, 2003.

Satjipto Rahardjo, *Hukum dan Perubahan Sosial ,* Bandung : Alumni , 1983

Satjipto Rahardjo, *Ilmu Hukum*, Bandung: PT. Citra Aditya Bakti, 2014.

Soerjono Soekanto, *Faktor – Faktor yang Mempengaruhi Penegakan Hukum*, Edisi Revisi, Jakarta: RajaGrafindo Persada, 2012.

Soerjono Soekanto, *Pengantar Penelitian Hukum*, Cet. Ke-3, Jakarta: Penerbit Universitas Indonesia (UI Press), 2006.

Soerjono Soekarto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Rajawali Pers, Jakarta, 2011.

Soesilo, R, Kitab Undang-undang Hukum Pidana (KUHP), Politeia, Bogor, 1991

Sutan Remy Sjahdeini, *Kebebasan Berkontrak dan Perlindungan Yang Seimbang Bagi Para Pihak Dalam Perjanjian Kredit Bank Di Indonesia,* Jakarta: Pustaka Utama Grafiti, 2009.

Sutan Remy Syahdeini, *Kejahatan & Tindak Pidana Komputer*, Jakarta: Pustaka Utama Grafiti, 2009.

Teguh Prasetyo, *Hukum Pidana*, Raja Grafindo Persada, Jakarta,2010.

Theo Huijbers, *Filsafat Hukum Dalam Lintasan Sejarah*, Jogyakarta:Kanisius,1982

Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta

Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-undang Nomor 7 Tahun 1992 tentang Perbankan. Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia.

Undang-undang Nomor 8 Tahun 1981 Kitab Undang-Undang Hukum acara Pidana.

Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP Jilid I dan II*, Jakarta, Pustaka Kartini, 1988 dan 1993.

Yanto awaludin, *Undang-Undang Informasi Dan Transaksi Elektronik,* http://selalucintaindonesia.wordpress.com/2013/01/15/undang-undang-informasi-dan-transaksi- elektronik/, 2013.

DAFTAR RIWAYAT HIDUP

Data Pribadi

Nama	:	Beni Setiawan
Tempat/tanggal lahir	:	Magetan, 16 Desember 1993
Jenis Kelamin	:	Laki-laki
Alamat/phone/hp/e-mail	:	Desa Sungai Rambai, Kec. Senyerang, Kab. Tanjung Jabung Barat - Jambi 085378038025 Benysetiawan077@gmail.com
Status	:	Belum menikah
Agama	:	Islam
Kewarganegaraan	:	Indonesia

Pendidikan Formal

2000 - 2006	:	SD Negeri Nguri IV, Kec. Lembeyan Kab. Kabupaten Magetan Jawa Timur
2006 - 2009	:	SMP Negeri 1 Lembeyan, Kec. Lembeyan Kab. Kabupaten Magetan Jawa Timur
2009 - 2011	:	Jurusan Pemasaran - SMK Negeri 1 Kuala Tungkal, Kab. Tanjung Jabung Barat-Jambi
2012 - 2016	:	S1 pada Program Studi Perbandingan Mazhab dan Hukum Institut Agama Islam Negeri Sultan Thaha Syaifuddin Jambi
2017 – Sekarang	:	S2 pada Program Magister Ilmu Hukum Universitas Batanghari Jambi

Pendidikan Non formal

2006	:	Kursus Bahasa Inggris pada Kampung Inggris Jambi

Prestasi Akademik

Indeks Prestasi Kumulatif	:	3.57 (0 – 4)
Judul Skripsi	:	Sanksi Pidana Mati Terhadap Bandar Narkotika (Studi Komparatif Fatwa MUI Nomor 53 Tahun 2014 dan Undang-undang Nomor 35 Tahun 2009)

Pengalaman Kerja

2016 - Sekarang	:	Staf Akademik/Staf IT Pangkalan Data PDDIKTI dan EMIS Institut Agama Islam Nusantara Batang Hari
2017 - Sekarang	:	Pengelola Jurnal Attasyrih dan Jurnal Muammalah
2018 - Sekarang	:	Pengelola Jurnal JISEC (*Journal Islamic Student Education Childhood*)
2017- Sekarang	:	Asisten Dosen pada Institut Agama Islam Nusantara Batang Hari.

Pengalaman Organisasi

2009 - 2010	:	Anggota MPK Osis SMK N 1 Kuala Tungkal
2010 – 2011	:	Dewan Ambalan Pangeran Diponegoro Gerakan Pramuka GUDEP SMK N 1 Kuala Tungkal
2010 - 2012	:	Dewan Kerja Cabang Kwartir Cabang Gerakan Pramuka Tanjung Jabung Barat.
2010 - 2011	:	Dewan Saka Wanabakti Gerakan Pramuka Saka Wanabakti Dinas Kehutanan Tanjung Jabung Barat
2014 - 2015	:	Sekretaris Pengurus Himpunan Mahasiswa Jurusan Perbandingan Mazhab da Hukum IAIN STS Jambi
2015 - 2016	:	Anggota Pengurus Pusat Persatuan Mahasiswa Perbandingan Mazhab seluruh Indonesia
2017-Sekarang	:	Pengelola Galeri Investasi Syariah Bursa Efek Indonesia di IAI Nusantara Batanghari
2018- sekarang	:	Anggota Pengelola Jurnal Ilmiah Pendidikan Islam Anak Usia Dini Se- Indonesia
2019-sekarang	:	Pembina Korps Sukarela Palang Merah Indonesia IAI Nusantara Batang Hari

Penelitian

2019	:	Upaya Literasi Dalam Peningkatan Sumber Daya Peserta Didik di Kabupaten Batang Hari