TESIS

KEBIJAKAN FORMULASI PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU KEJAHATAN *CYBERSQUATTING*

THE POLICY ON THE FORMULATION OF CRIMINAL RESPONSIBILITY AGAINST CYBERSQUATTING PERPETRATORS

DEWI MUTI'AH, S.H
160720101001

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS JEMBER
FAKULTAS HUKUM
MAGISTER HUKUM
2018

TESIS

KEBIJAKAN FORMULASI PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU KEJAHATAN *CYBERSQUATTING*

THE POLICY ON THE FORMULATION OF CRIMINAL RESPONSIBILITY AGAINST CYBERSQUATTING PERPETRATORS

DEWI MUTI'AH, S.H
160720101001

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS JEMBER
FAKULTAS HUKUM
MAGISTER HUKUM
2018

KEBIJAKAN FORMULASI PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU KEJAHATAN *CYBERSQUATTING*

THE POLICY ON THE FORMULATION OF CRIMINAL RESPONSIBILITY AGAINST CYBERSQUATTING PERPETRATORS

TESIS

Untuk memperoleh Gelar Magister dalam Program Studi Magister Ilmu Hukum
Pada Program Pascasarjana Universitas Jember

Oleh:

DEWI MUTI'AH, S.H
160720101001

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS JEMBER
FAKULTAS HUKUM
MAGISTER HUKUM
2018

PERSETUJUAN

TESIS INI TELAH DISETUJUI

TANGGAL 17 MEI 2018

Oleh:

Dosen Pembimbing Utama,

Prof. Dr. M. ARIEF AMRULLAH, S.H., M.Hum.
NIP: 196001011988021001

Dosen Pembimbing Anggota

Dr. FANNY TANUWIJAYA, S.H., M.Hum
NIP: 196506031990022001

PENGESAHAN

KEBIJAKAN FORMULASI PERTANGGUNGJAWABAN PIDANA

TERHADAP PELAKU KEJAHATAN *CYBERSQUATTING*

Oleh:

DEWI MUTI'AH, S.H.
NIM: 160720101001

Dosen Pembimbing Utama	Dosen Pembimbing Anggota
Prof. Dr. M. ARIEF AMRULLAH,S.H., M.Hum	**Dr. FANNY TANUWIJAYA,S.H.,M.Hum**
NIP. 196001011988021001	**NIP. 196506031990022001**

Mengesahkan,
Program Studi Magister Hukum
Fakultas Hukum
Universitas Jember
Dekan,

Dr. NURUL GHUFRON, S.H., M.H.
NIP. 197409221999031003

PENETAPAN PANITIA PENGUJI

Dipertahankan dihadapan Panitia Penguji pada:

Hari : Sabtu

Tanggal : 26

Bulan : Mei

Tahun : 2018

Diterima oleh Panitia Penguji Fakultas Hukum Universitas Jember:

Ketua	**Sekretaris**
Dr. Y.A. Triana Ohoiwutun, S.H., M.H	**Dr. Ermanto Fahamsyah, S.H., M.H**
NIP: 196310131990032001	**NIP: 197905142003121002**

ANGGOTA PENGUJI:

Dr. Jayus, S.H.,M.Hum. **: (.....)**
NIP: 195612061983031003

Prof. Dr. M. Arief Amrullah, S.H., M.Hum. **: (.....)**
NIP: 196001011988021001

Dr. Fanny Tanuwijaya, S.H., M.Hum. **: (.....)**
NIP: 196506031990022001

PERNYATAAN ORISINALITAS TESIS

Dengan ini saya menyatakan bahwa:

1. Tesis ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (Magister Hukum), baik di Universitas Jember maupun di perguruan tinggi lain.
2. Tesis ini merupakan hasil dari gagasan, ide, pemikiran, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan dari Tim Pembimbing.
3. Dalam Tesis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan maupun daftar pustaka.
4. Apabila ternyata dalam naskah tesis ini dapat dibuktikan adanya unsur-unsur jiplakan, maka saya bersedia menerima sanksi akademik maupun sanksi lainnya yang berlaku di lingkungan Universitas Jember.

Jember, 04 Mei 2018

Yang membuat pernyataan,

DEWI MUTI'AH, S.H
NIM: 160720101001

UCAPAN TERIMAKASIH

Syukur Alhamdulillah, segala Puja dan Puji syukur Penulis panjatkan kepada Allah S.W.T, Tuhan Yang Maha Pengasih Lagi Maha Penyayang atas segala Rahmat, Petunjuk, serta Hidayah yang telah diberikan, sehingga penulis dapat menyelesaikan tesis dengan judul: kebijakan formulasi pertanggungjawaban pidana terhadap pelaku kejahatan *cybersquatting*; penulisan tesis ini merupakan tugas akhir sebagai syarat untuk menyelesaikan Program Studi Magister Hukum pada Fakultas Hukum Universitas Jember serta mencapai gelar Magister Hukum periode tahun 2018. Pada kesempatan ini mengucapkan terimakasih kepada pihak-pihak yang telah banyak membantu dan memberikan dukungan dalam penulisan tesis ini, antara lain:

1. Prof. Dr. M. Arief Amrullah, S.H., M.Hum, selaku Dosen Pembimbing Utama penyusunan tesis;
2. Dr. Fanny Tanuwijaya, S.H., M.Hum, sebagai Dosen Pembimbing Anggota penyusunan tesis;
3. Dr. Y.A. Triana Ohoiwutun, S.H., M.H, selaku Kaprodi Pascasarjana Fakultas Hukum Universitas Jember;
4. Dr. Ermanto Fahamsyah, S.H., M.H, selaku sekretaris penguji tesis;
5. Dr. Jayus, S.H., M.Hum, selaku Dosen Penguji tesis;
6. Dr. Nurul Ghufron, S.H., M.H, selaku Dekan Fakultas Hukum Universitas Jember, Dr. Dyah Octorina Susanti, S.H., M.Hum, selaku Penjabat Wakil Dekan I Fakultas Hukum Universitas Jember, Echwan Iriyanto, S.H.,M.H selaku Penjabat Wakil Dekan II Fakultas Hukum Universitas Jember, dan Dr. Aries Harianto, S.H.,M.H, selaku Penjabat Wakil Dekan III Fakultas Hukum Universitas Jember.
7. Bapak dan Ibu dosen, civitas akademika, serta seluruh karyawan Fakultas Hukum Universitas Jember atas segala ilmu dan pengetahuan yang diberikan;
8. Orang tua saya, semua keluarga dan kerabat atas do’a dan dukunngan yang telah diberikan dengan setulus hati;

9. Teman-teman seperjuangan di Program Magister Hukum Fakltas Hukum Universitas Jember angkatan tahun 2016 yang tidak dapat saya sebutkan satu persatu yang telah memberikan dukunngan dan bantuan baik moril dan spirituil;
10. Semua pihak dan rekan-rekan yang tidak dapat disebutkan satu-persatu yang telah memberikan bantuannya dalam penyusunan tesis hukum ini.

Menyadari sepenuhnya akan keterbatasan penulis baik dari segi kemampuan dan keterbatasan bekal ilmu saat menulis tesis ini. Oleh karena itu, senantiasa penulis akan menerima segala kritik dan saran dari semua. Akhirnya penulis mengharapkan, mudah-mudahan tesis ini minimal dapat menambah khasanah refrensi serta bermanfaat bagi pembaca sekalian.

Jember, Mei 2018

Penulis,

DEWI MUTI'AH, S.H

NIM: 160720101001

MOTTO

"Jangan kau katakan saya tidak dapat,

Tetapi katakan saya mau"

(R.A. Kartini)

Ahmad Nurcholish, *Celoteh R. A. Kartini (232 Ujaran Bijak Sang Pejuang Emansipasi)*, 1st ed (Jakarta: PT. Elex Media Komputindo, 2018). Hlm.74

RINGKASAN

Era globalisasi sekarang ini telah menyebabkan terjadinya perkembangan di berbagai sektor, salah satunya ialah sektor teknologi. perkembangan yang paling signifikan dalam dunia teknologi ialah hadirnya komputer yang kemudian melahirkan suatu hal baru yang dikenal dengan *internet*. Berjalannya waktu *internet* telah menjadi suatu kebutuhan pokok yang sangat digemari bagi seluruh masyarakat di dunia. Tidak dapat dipungkiri bahwa lahirnya *internet* seperti pedang bermata dua, di satu sisi memberikan dampak positif dan di sisi lain menimbulkan dampak negatif. Dampak negatif yang ditimbulkan dari adanya *internet* ialah munculnya kejahatan-kejahatan baru yang berkaitan dengan *internet* dan menyebabkan persoalan-persoalan hukum baru, seperti timbulnya kejahatan *cybersquatting*. *Cybersquatting* adalah suatu kejahatan yang berkaitan dengan nama domain. Nama domain adalah alamat yang digunakan dalam *internet*, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam *internet*. Pelaku kejahatan *cybersquatting* memanfaatkan nama domain terkenal yang kemudian membuat duplikat dan mendaftarkannya untuk dijual kembali kepada yang berhak atas nama domain tersebut dengan harga yang lebih tinggi. Hukum positif Indonesia saat ini masih belum mengatur secara khusus mengenai kejahatan *cybersquatting*, hal itu mengakibatkan pelaku kejahatan *cybersquatting* sulit untuk dibebankan pertanggungjawaban secara pidana dikarenakan tidak diaturnya dalam hukum positif Indonesia. Apabila hukum positif yang ada saat ini dipaksakan untuk diterapkan pada kejahatan *cybersquatting* maka hal tersebut akan bertentangan dengan asas legalitas dalam hukum pidana. Berdasarkan uraian di atas permasalahan yang dibahas ada 2 (dua) yaitu: *pertama*, apakah Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dapat diterapkan dalam sistem pertanggungjawaban pidana terhadap pelaku *cybersquatting*?, *kedua*, bagaimanakah kebijakan formulasi yang ideal dalam pertanggungjawaban terhadap pelaku kejahatan *cybersquatting*?

Metode penulisan yang digunakan penulis adalah yuridis normatif. Pendekatan masalah yang digunakan adalah pendekatan Undang-Undang *(statue approach)*, pendekatan konseptual *(conceptual approach)*, pendekatan perbandingan *(comparative approach)*, dan pendekatan historis *(historial approach)*. Bahan sumber hukum yang digunakan adalah bahan hukum primer dan bahan hukum sekunder. Tujuan penelitian ini adalah untuk mengkaji dan menganalisis pertanggungjawaban pidana terhadap pelaku kejahatan c*ybersquatting* dalam Undang-Undang Informasi dan Transaksi Elektronik, serta untuk menentukan kebijakan formulasi yang ideal dalam pertanggungjawaban terhadap pelaku kejahatan *cybersquatting*.

Hasil kajian yang diperoleh bahwa: *Pertama.* Teori kesalahan yang terdapat dalam pertanggungjawaban pidana memberikan beban pada korban untuk membuktikan bahwa pelaku melakukan perbuatan yang melawan hukum. Teori tersebut pada dasarnya telah dianut oleh Undang-Undang ITE. Terkait pertanggungjawaban pelaku dalam kejahatan *cybersquatting* berlaku adanya kesalahan. Akan tetapi, pertanggungjawaban pidana dalam Undang-Undang ITE

saat ini tidak dapat diterapkan terhadap kejahatan *cybersquatting*. Hal tersebut dikarenakan belum diatur nya kejahatan *cybersquatting* dalam Undang-Undang ITE dan berakibat pelaku kejahatan *cybersquatting* tidak dapat dipertanggungjawabkan atas perbuatannya. Apabila Undang-Undang ITE diterapkan terhadap pelaku kejahatan *cybersquatting* jelas akan bertentang dengan asas legalitas. Indonesia dapat juga mencontoh Amerika Serikat dalam hal pertanggungjawaban terhadap pelaku kejahatan *cybersquatting*. Jika Amerika hanya memberikan pertanggungjawaban berupa denda, maka Indonesia dapat menambahkan pidana penjara terhadap pelaku untuk memberikan efek jera dan rasa takut bagi para pelaku selanjutnya. *Kedua.* Teori anomie yang dikemukan oleh durkheim menyatakan bahwa suatu kejahatan itu muncul karena tidak ada norma yang mengaturnya. Oleh karena itu sangat diperlukan suatu kebijakan formulasi terhadap kejahatan *cybersquatting.* Kebijakan formulasi pertanggungjawaban pidana yang ideal terhadap pelaku kejahatan *cybersquatting* di masa yang akan datang telah tercantum dalam RKUHP Tahun 2015 dan RKUHP Tahun 2017 melalui proses kriminalisasi terhadap kejahatan *cybersquatting* dengan menentukan aturan mengenai sistem pidana dan pemidanaannya, sehingga pertanggungjawaban pidana dapat dibebankan kepada pelaku kejahatn *cybersquatting*. Seiring dengan proses kriminalisasi terhadap kejahatan *cybersquatting*, maka tidak terdapat pelanggaran asas legalitas dalam penerapannya kelak.

Berdasarkan hasil kajian tersebut penulis memberikan saran, antara lain: *Pertama*. Hukum positif Indonesia saat ini masih mempunyai keterbatasan dalam hal pertanggungjawaban pidana terhadap pelaku kejahtan *cybersquatting* dikarenakan Undang-Undang ITE yang ada saat ini tidak memadai untuk diaplikasikan terhadap kejahatan *cybersquatting*, jadi diperlukan suatu pembaharuan terhadap Undang-Undang ITE. *Kedua.* Perlu segera dibahas dan disahkan mengenai RKUHP supaya pertanggungjawaban pidana dapat dibebankan kepada pelaku kejahatan *cybersquatting* dan untuk meningkatkan kemampuan hukum pidana dalam pemberantasan kejahatan *cybersquatting* di Indonesia.

SUMMARY

The era of globalization has now led to the development of various sectors, one of which is the technology sector. the most significant development in the world of technology is the presence of computers that then gave birth to a new thing known as the internet. The passage of internet time has become a very popular necessity for all people in the world. It can not be denied that the birth of the internet like a double-edged sword, on the one hand gives a positive impact and on the other side a negative impact. Negative impacts caused by the internet are the emergence of new internet-related crimes and causing new legal issues, such as the incidence of cybersquatting crimes. Cybersquatting is a crime associated with the name of the domain. The domain name is the address used in the internet, which is a unique code or character arrangement to indicate a particular location on the internet. Cybersquatting criminals take advantage of well-known domain names which then make duplicates and register them for resale to those eligible for the domain name at a higher price. Indonesia's current positive law still has not specifically regulated the crime of cybersquatting, it has resulted in cybersquatting criminals difficult to be criminally liable due to the non-regulation in Indonesian positive law. If the current positive law is enforced to apply to cybersquatting crimes then it will be contrary to the legality principle of the criminal law. Based on the above description of the issues discussed there are 2 (two), namely: first, whether Law Number 19 Year 2016 on Information and Electronic Transactions can be applied in the system of criminal liability to cybersquatting perpetrators ?, second, what is the ideal formulation policy in accountability against cybersquatting criminals?

Writing method used by writer is normative juridical. The problem approach used is the statue approach, the conceptual approach, the comparative approach, and the historical approach. The legal source materials used are primary legal materials and secondary legal materials. The purpose of this study is to examine and analyze criminal liability for ybersquatting criminals in the Information and Electronic Transactions Act, as well as to determine the ideal formulation policy in accounting against cybersquatting offenders.

The results of the study obtained that: First. The error theory contained in criminal responsibility places a burden on the victim to prove that the perpetrator is committing an unlawful act. The theory has been fundamentally embraced by the ITE Act. Regarding the liability of the perpetrator in cybersquatting crime there is an error. However, criminal liability in the current ITE Act is not applicable to cybersquatting crimes. This is because the cybersquatting crime has not been regulated in the ITE Act and resulted in cybersquatting criminals can not be accounted for his actions. If the ITE Act applied to cybersquatting criminals clearly will be contrary to the principle of legality. Indonesia can also emulate the United States in terms of accountability against cybersquatting offenders. If the United States only provides liability in the form of fines, then Indonesia can add imprisonment to the perpetrators to provide a deterrent effect and fear for subsequent perpetrators. Second. The anomie theory brought by Durkheim states that a crime arises because there is no norm

governing it. Therefore it is necessary a formulation policy against cybersquatting crimes. The ideal criminal responsibility formulation policy against future cybersquatting offenders has been listed in the RKUHP of 2015 and RKUHP 2017 through the criminalization process of cybersquatting crimes by determining the rules of the criminal system and its punishment, so that criminal liability may be imposed on cybersquatting perpetrators. Along with the criminalization process of cybersquatting crime, there is no violation of the principle of legality in the future.

Based on the results of this study the authors provide suggestions, among others: First. Indonesia's current positive law still has limitations on criminal liability for perpetrators of cybersquatting because the existing ITE Act is inadequate to apply to cybersquatting crimes, so a renewal of our ITE Act is required. Second. It needs to be discussed and ratified immediately about the Criminal Code so that criminal responsibility can be charged to cybersquatting criminals and to improve criminal law ability in eradicating cybersquatting crime in Indonesia.

DAFTAR ISI

GLOSARIUM

ACPA	:*Anti Cybersquatting Consumer Protection Act* suatu lembaga yang berada di Amerika Serikat yang bertujuan untuk memperluas sarana perlindungan merek dagang untuk memenuhi celah hukum yang ada.
Blackmailing	:Pemerasan yang dilakukan melalui dunia elektronik atau virtual.
Booting	:Proses pemasukan arus listrik kedalam peralatan komputer sehingga komputer dapat berkomunikasi dengan pengguna.
Cracking	:Kegiatan membobol suatu sistem komputer dengan tujuan untuk mengambil sistem tersebut.
Cyberspace	:Media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal-balik secara *online* (terhubung langsung)
Cybersquatter	:Orang atau pihak yang melakukan kejahatan *cybersquatting*
Cybersquatting	:Kejahatan yang dilakukan dengan cara mendaftarkan nama domain perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal
Dropcatcher	:Perbuatan registrasi ulang nama domain yang sudah kadaluwarsa untuk menghindari seseorang membeli nama domain tersebut.
Domainer	:Penyalur nama domain, yang menghasilkan uang dari membeli dan menjual nama domain.
Domain Name	:Dalam bahasa Indonesia lebih dikenal dengan nama domain, ialah alamat *internet* yang dapat digunakan untuk berkomunikasi dalam *internet*, yang berupa kode atau

susunan karakter yng bersifat unik untuk menunjukkan lokasi tertentu dalam *internet*.

Domain Parking :Perbuatan yang dapat menghasilkan uang dengan cara memiliki situs-situs kecil yang hanya menautkan ilkan ke domain tersebut, dimana pemilik membayar sejumlah kecil setiap kali seseorang mengklik iklan tersebut, yang berakibat *cybersquatter* memperoleh hingga jutaan dalam beberapa kasus.

Domain Tasting :Praktek percobaan domain untuk periode tertentu dengan pengembalian uang gratis dalam lima hari pengujian, kemudian menjatuhkan untuk mengembalikan uang yang tidak berjalan dengan baik.

Phising :Suatu metode yang digunakan *hacker* untuk mencuri password dengan cara mengelabui target menggunakan fake form login pada situs plasu yang menyerupai situs asli.

Hacker :Orang yang mempelajari, menganalisa, memodifikasi, atau bahkan mengeksploitasi sistem yang terdapat di sebuah perangkat seperti perangkat lunak komputer dan perangkat keras komputer seperti program komputer, administrasi, dan hal-hal lainnya terutama pada sistem keamanan.

Hacking :Kegiatan memasuki sistem melalui sistem operasional lain yang dijalankan oleh *hacker* dengan tujuan mencari titik keamanan pada sistem yang akan dimasuki.

ICANN :*Internet Corporation for Assigned Name and Number*, suatu organisasi yang dibentuk yang dibentuk pada tahun 1998 sebagai organisasi nirlaba yang berfungsi sebagai pengawasan terhadap kebijakan sistem pendaftaran nama domain

Inter NIC	:*Internet Network Information Center* suatu lembaga yang didirikan untuk melayani pendaftaran nama domain.
Network Solution	:Suatu organisasi yang didirikan pada tahun 1979 dan berbasis di Amerika serikat, dan bergerak dalam bidang pendaftaran nama domain.
PANDI	:Suatu lembaga yang dibentuk oleh pemerintah Indonesia pada 29 Desember 2006 untuk mengatur engenai nama domain di Indonesia
Registrant	:Nama penilik sebuah domain
Registrar	:Pihak yang memiliki kewenangan dalam melakukan proses pendaftaran, renewal dan transfer domain
Spamming	:Kegiatan mengirim email palsu dengan memanfaatkan server email yang memiliki "smtp open relay" atau dapat juga diartikan dengan pengiriman informasi atau iklan suatu produk yang tidak pada tempatnya.
Typosquatter	:Orang atau pihak yang melakukan *typosquatting*
Typosquatting	:Sering disebut dengan pembajakan URL. Hal tersebut terjadi pada saat pengguna internet membuat kesalahan ketik ketika memasukkan alamat web ke browser web. Setelah pengguna mengetikkan alamat yang salah dan akhirnya mengarah pada situs web pengganti yang dibuat oleh *cybersquatter*.
UDRP	:Suatu lembaga yang dibentuk oleh *ICANN* pada tahun 1999 yang bertujuan untuk menyelesaikan kasus-kasus yang berhubungan dengan nama domain dan direkomendasikan oleh *ICANN*.
URL	:*Uniform Resource Locator* ialah rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber seperti dokumen dan gambar diinternet.

WIPO	:Salah satu lembaga khusus yang didirikan pada tahun 1967 yang mengatur mengenai hak milik intelektual.

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Era globalisasi sekarang ini menyebabkan terjadinya perkembangan di berbagai sektor, salah satunya ialah sektor teknologi. Perkembangan yang paling signifikan dan pesat dalam sektor teknologi ialah komputer. Seiring berjalannya waktu, komputer terus berkembang dan melahirkan suatu hal baru yang kita kenal dengan nama *Internet. Internet* adalah sebuah jaringan yang mampu mengkoneksikan antar sub-sistem jaringan menjadi satu jaringan yang sangat besar yang saling terhubung satu sama lain di seluruh dunia.[1] Seiring berjalannya waktu, *internet* telah berubah menjadi kebutuhan pokok yang sangat digemari bagi seluruh masyarakat di dunia, mulai dari masyarakat biasa, pelajar, hingga pegawai atau pejabat pemerintahan memanfaatkan *internet* untuk kegiatannya sehari-hari.

Tidak dapat dipungkiri bahwa munculnya *internet* diibaratkan pedang bermata dua, di satu sisi memberikan dampak positif dan di sisi lain menimbulkan dampak negatif. Dampak positif dari adanya *internet* ialah kita dapat memperoleh berbagai informasi di seluruh dunia dengan mudah. Selain itu, adanya *e-mail* dan media sosial seperti *facebook, twitter, skype*, dan lain-lain telah memberikan kemudahan kepada kita untuk berkomunikasi tanpa dibatasi oleh jarak. Seiring dengan perkembangan *internet* yang semakin pesat, muncul kejahatan-kejahatan

[1] Widodo, *Hukum Pidana di Bidang Teknologi Informasi. Cybercrime Law: Telaah Teoritik dan Bedah Kasus*, 1st ed (Yogyakarta: Aswaja Pressindo, 2013). Hlm.v

yang berkaitan dengan *internet* dan menyebabkan persoalan-persoalan hukum baru yang terjadi dalam berbagai bidang.

Perkembangan *internet* selanjutnya ditandai dengan didirikannya suatu lembaga yang mengurus tentang pengelolaan nama domain yang dikenal dengan *InterNIC* pada tahun 1993 dengan prinsip pelayanan *first-come-first-served*.[2] Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (untuk selanjutnya disebut dengan Undang-Undang ITE) Pasal 1 angka 20 memberikan pengertian mengenai nama domain. Nama domain adalah alamat *internet* penyelenggaran negara, orang, badan usaha, dan/atau masyarakat, yang dapat digunakan untuk berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam *internet.* Kenyataannya, penggunanan nama domain sering disalahgunakan oleh pihak-pihak tertentu dengan tujuan ingin mendapat keuntungan yang besar dari nama domain tersebut. Permasalahan nama domain berkaitan dengan fungsi nama domain itu sendiri yaitu sebagai alamat di *internet*. Selain itu, penamaan terhadap nama domain juga berkaitan dengan suatu perusahan atau suatu produk yang sering kali dijadikan *trademark* dari perusahaan atau produk tersebut. Perusahaan atau produk tersebut biasanya telah mempunyai reputasi yang bagus dan dikenal masyarakat luas.

Penyalahgunaan terhadap nama domain telah menimbulkan suatu kejahatan baru dalam dunia *cyber*, yaitu *cybersquatting*. Para pelaku kejahatan

[2] Sabartua Tampubolon, *Aspek Hukum Nama Domain di Internet*, 1st ed (Jakarta: PT. Tatanusa, 2003). Hlm.4

memanfaatkan nama domain terkenal dengan cara membuat duplikat dari nama domain tersebut yang kemudian mendaftarkannya untuk dijual kembali pada pihak lain dengan harga yang lebih tinggi. Dengan kata lain, *Cybersquatting* adalah praktek-praktek oleh para pihak-pihak tertentu untuk mendahului mendaftarkan suatu nama domain tertentu yang terkait dengan perusahaan lain tertentu dengan tujuan memperoleh keuntungan dengan cara menjual nama domain tersebut kepada perusahaan yang seharusnya memiliki nama domain tersebut.[3]

Sebagaimana ditulis dalam *International Journal of Law and Information Technology*:[4]

> *Cybersquatting is a particular type of domain name dispute which occurs when someone registers a domain which is associated with a famous firm with the sole intention of selling it on to them at a higher price* (*Terjemahan penulis. *Cybersquatting* adalah salah satu jenis kejahatan yang berupa sengketa nama domain yang terjadi pada saat seseorang mendaftarkan nama domain tersebut yang dikaitkan dengan nama perusahaan terkenal dengan tujuan menjual nama domain tersebut kepada perusahaan yang bersangkutan dengan harga yang lebih tinggi).

Cybersquatting sendiri dalam Peraturan dan organisasi Internasional telah diatur dalam *Anti-Cybersquatting Consumer Protection Act (ACPA)* dan *Uniform Dispute Resolution Policy (UDRP)*. *ACPA* dikeluarkan pada pemerintahan Clinton pada 29 November 1999 yang bertujuan untuk *to extend the exisiting means of trademark protection to "non-famous" marks. The concept of "distinctive" marks comes to fill an important legal gap* (*terjemanhan penulis. Untuk memperluas

[3] *Ibid*. Hlm.46
[4] M Moore, *"Cybersquatting: Prevention better than cure?"* (2009) 17:2 Int J Law Inf Technol 220.

sarana perlindungan merek dagang. Konsep tersebut untuk memenuhi celah hukum yang ada).[5] Organisasi Internasional selanjutnya yang mengatur mengenai nama domain dan *cybersquatting* ialah *UDRP*. *UDRP* merupakan forum arbitrase yang disahkan pada tanggal 24 Oktober 1999. Ketentuan dalam *UDRP* hampir sama dengan *ACPA*, hanya saja prosedur dalam *UDRP* lebih fleksibel, lebih singkat, dan lebih murah.[6] Indonesia sendiri telah memiliki suatu lembaga yang mengatur mengenai nama domain yaitu PANDI (Pengelola Nama Domain Internet Indonesia). PANDI dibentuk pada 29 Desember 2006 oleh pemerintah Indonesia yang tujuan utamanya adalah mengelola nama domain di Indonesia.[7]

Pada kenyataannya, meskipun terdapat organisai dan peraturan yang mengatur mengenai *cybersquatting* dan nama domain, masih terdapat kejahatan yang berhubungan dengan nama domain khususnya *cybersquatting*, baik diluar negeri maupun di Indonesia. Kejahatan *cybersquatting* yang terjadi di Indonesia ialah kasus mustikaratu.com, kasus sengketa chanel5.com dan yang paling baru ialah kasus traveloka. Kasus mustikaratu.com banyak mendapat perhatian di Indonesia dan sempat diproses ke Pengadilan Jakarta Pusat, meskipun pada akhirnya kasus tersebut ditolak oleh hakim karena tidak memenuhi unsur-unsur yang didakwakan Jaksa Penuntut Umum yang kemudian putusan tersebut dianulir oleh Mahkamah Agung.[8]

Kasus mustikaratu.com berawal saat tersangka Tjandra Sugiono diangkat menjadi General Marketing Internasional PT. Martino Berto yang merupakan

---

[5] Tampubolon, *Op.Cit*. Hlm.66
[6] *Ibid*. Hlm.68
[7] "Tentang Pandi", online: <https://pandi.id/profil/tentang-pandi/>.
[8] Tampubolon, *Op.Cit*. Hlm.92

perusahaan milik Ny. Martha Tilaar. Pada tanggal 7 Oktober 1999 tersangka mendaftarkan nama domain Mustika-ratu.com ke *Network Solution.* Setelah mendaftarkan nama domain tersebut tersangka kemudian mengundurkan diri dari PT. Martina Berto. Pada saat pihak PT. Mustika Ratu ingin mendaftarkan nama domain miliknya ke *Network Solution*, ternyata telah ada yang mendaftarkan nama domain tersebut atas nama tersangka. Karena merasa dirugikan, pihak PT. Mustika Ratu melaporkan kasus tersebut ke Korps Reserse Polri. Atas laporan tersebut akhirnya tersangka mencabut nama domain Mustika-ratu.com dan *Network Solution*. Namun karena merasa dirugikan, pihak PT. Mustika Ratu tetap melanjutkan tuntutannya. Sengketa nama domain tersebut telah membuat PT. Mustika Ratu rugi sebesar kurang lebih 10 milyar rupiah. Serta, menyebabkan banyak pelanggan PT. Mustika Ratu yang berada di luar negeri tidak dapat mengakses *website* milik PT. Mustika Ratu. Bahkan, para pelanggan menjadi bingung karena masuk ke *website* http://www.belia.com yang memasarkan produk dari PT. Martina Berto yaitu Sariayu.[9]

Kejahatan *cybersquatting* juga terjadi pada traveloka.com. Co-founder traveloka, Ferry Unardi menyatakan bahwa seseorang telah membeli beberapa nama domain yang berhubungan dengan traveloka kemudian menghubungkannya ke dalam situs porno lokal bernama krucil2. Co-founder traveloka menyatakan bahwa, meskipun mereka telah mendaftarkan merek dagang dengan nama "traveloka", tetapi mereka tidak dapat melakukan apa-apa. Hal tersebut

[9] *Ibid*. Hlm.93-94

disebabkan karena privasi pemilik domain-domain tersebut dilindungi serta pihak traveloka tidak mengatahui siapa pelaku sebenarnya.[10]

Berbeda dengan dua kasus diatas yang korban dan pelakunya merupakan WNI. Beberapa kasus ini melibatkan WNA baik sebagai korban maupun sebagai pelaku. Salah satunya ialah kasus sengketa channel5.com. Kasus ini bermula dari *Channel 5 Broadcasting Ltd* yang mengajukan komplain kepada *National Arbitration Forum* mengenai pendaftaran nama domain channel5.com oleh *respondent* dalam hal ini PT. Pancawana Indonesia, melalui *registrat* IARegistry.com.[11]

Kasus ini melibatkan PT. Pancawana Indonesia perusahaan teknologi informasi Indonesia yang berasal di Jawa Tengah yang mendaftarkan channel5.com. perusahaan tersebut digugat oleh *Channel 5 Broadcasting Ltd,* perusahaan penyiaran asal Inggris. Kasus ini menjadi menarik karena tindakan Sahar Sarid yang mengklaim bertindak atas nama PT. Pancawana Indonesia, mengaku bahwa pihaknya pemilik merk *"channel5.com"* yang telah didaftarkan di Ditjen HKI (Hak Kekayaan Intelektual). Tapi pada akhirnya, sengketa nama domain ini dimenangkan oleh pihak *Channel 5 Broadcasting Ltd* dan nama domain channel5.com harus dialihkan kepada *Channel 5 Broadcasting Ltd.*[12]

Penyelesaian kasus *Channel 5 Broadcasting* di atas diselesaikan melalui aribtrase yang dilakukan oleh ICANN *(Internet Corporation for Assigned Name*

---

[10] Yoga Tri Priyanto, "Kontroversi cybersquatting menyerang Indonesia dan Traveloka", (12 November 2003), online: *Kontroversi Cybersquatting Menyerang Indones Dan Travel* <https://www.merdeka.com/teknologi/kontroversi-cybersquatting-menyerang-indonesia-dan-traveloka.html>. (diakses pada tanggal 16 Oktober 2017, Pukul 09.00 wib)

[11] Tampubolon, *Op.Cit*. Hlm.99

[12] *Ibid*. Hlm.99-101

and Number). ICANN adalah satu organisasi yang dibentuk pada Oktober 1998 sebagai organisasi nirlaba yang berfungsi sebagai pengawasan terhadap kebijakan sistem pendaftaran nama domain. Berbeda dengan kasus *Channel 5 Broadcasting*, kasus Mustika Ratu telah sampai pada ranah peradilan. Tetapi dalam kasus Mustika Ratu tidak berdasarkan pada asas *lex specialis* karena menggunakan KUHP dalam penyelesaiannya. Hal tersebut menunjukkan bahwa peraturan hukum dalam dunia *cyber* berbanding terbalik dengan perkembangan kejahatan seiring dengan teknologi yang semakin berkembang.

Tidak dapat dipungkiri bahwa aktifitas dalam dunia *cyber* mempunyai spesifik sendiri yang tidak lagi patuh pada batasan-batasan teritorial dan hukum yang berlaku saat ini dianggap masih belum cukup memadai terhadap kasus-kasus *cyber* sekarang ini. Hal tersebut terjadi karena filosofi awal lahirnya Undang-undang ITE yang hanya mengatur mengenai transaksi elektronik saja dan tidak mengatur mengenai kejahatan dalam dunia *cyber*. Sehingga Undang Undang ITE tidak dapat mengimbangi kejahatan-kejahatan *cyber* yang semaking meningkat.

Munculnya segala perbuatan dalam dunia mayantara yang dapat merugikan orang lain, mendorong untuk dilakukannya kriminalisasi terhadap perbuatan-perbuatan tersebut. Hukum harus selalu berkembang agar dapat menjangkau perkembangan-perkembangan dalam teknologi. Aka tetapi, pada kenyataannya hukum masih jauh tertinggal dari perkembangan teknologi khususnya perbuatan-perbuatan yang terjadi dalam dunia mayantara. Sehingga, hukum masih belum mampu mengatasi permasalahan-permasalahan yang timbul dari kegiatan mayantara tersebut.

Dalam perkembangan hukum positif di Indonesia yang berlaku saat ini, tidak ada norma yang mengatur secara khusus mengenai kejahatan-kejahatan yang berkaitan dengan nama domain khususnya *cybersquatting*. Bahkan, Undang Undang ITE yang merupakan *Lex Specialis* juga tidak secara khusus mengatur mengenai kejahatan-kejahatan yang berkaitan dengan nama domain. Undang Undang ITE hanya memberikan penjelasan mengenai pengertian, pendaftaran, dan pengelolaan nama domain. Undang Undang ITE tidak mengatur secara khusus mengenai kejahatan *cybersquatting.* Sehingga jika terdapat kasus *cybersquatting* pihak penuntut umum memasukkan pasal-pasal KUHP dalam dakwaannya, dan penyelesaian seperti itu tidak berdasarkan hukum *lex specialis* yaitu Undang-undang ITE dan Undang-undang di luar KUHP yang sifat nya lebih khusus. Berdasarkan hal tersebut perlu adanya kebijakan formulasi yang mengatur mengenai kejahatan *cybersquatting* itu sendiri, sehingga jika terjadi kasus-kasus *cybersquatting* seperti diatas pelaku kejahatan dapat di pertanggungjawaban secara pidana.

Berdasarkan latar belakang yang telah diuraikan diatas maka sangat menarik untuk dibahas lebih lanjut dalam tesis yang berjudul **"Kebijakan Formulasi Pertanggungjawaban Pidana Terhadap Pelaku Kejahatan *Cybersquatting*"**

1.2 Rumusan Masalah

1. Apakah Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dapat diterapkan dalam sistem pertanggungjawaban pidana terhadap pelaku *cybersquatting*?

2. Bagaimanakah kebijakan formulasi yang ideal dalam pertanggungjawaban terhadap pelaku kejahatan *Cybersquatting*?

1.3 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penyusunan tesis hukum sebagaimana dirumuskan dalam rumusan masalah, yaitu:

1. Untuk mengkaji dan menganalisis pertanggungjawaban pidana terhadap pelaku kejahatan *cybersquatting* dalam Undang-undang Informasi dan Transaksi Elektronik;
2. Untuk menentukan kebijakan formulasi yang ideal dalam pertanggungjawaban terhadap pelaku kejahatan *cybersquatting*.

1.4 Manfaat Penelitian

Manfaat dari penelitian yang hendak dicapai dalam penyusunan tesis hukum ini adalah:

1. Penelitian ini diharapkan dapat memberikan masukan dan pengembangan dalam ilmu hukum dan hukum pidana secara umum, dan seacara khusus dapat menjadi pertimbangan dan kajian dalam menangani kejahatan *cybersquatting* yang saat ini masih belum jelas pengaturannya dalam peraturan perundang-undangan terutama dalam hal pertanggungjawabannya;
2. Menjadi dasar pertimbangan dan masukan bagi aparat penegak hukum untuk mendukung proses penegakan dalam hal penanganan terhadap kejahatan *cybersquatting* khususnya dalam hal pertanggungjawabannya.

1.5 Originalitas Penelitian

Karya ilmiah ini adalah hasil karya saya sendiri, kecuali jika disebutkan sumbernya dan belum pernah diajukan pada institusi manapun, serta bukan karya jiplakan. Penelitia ini pada dasarnya didasari oleh penelitian terdahulu dari beberapa tesis yang sejenis. Beberapa rujukan dan refrensi penelitian tesis hukum tersebut, adalah:

Bagian	**Alfred Nobel Sugio Hartono, Pascasarjana Universitas Atma Jata Yogyakarta, 2013**	**Muhammad Nizar, Pascasarjana Universita Airlangga Surabaya, 2017**	**Firda Laily Mufid, Pascasarjana Universitas Jember, 2017**
	(1)	(2)	(3)
Judul	Perlindungan Hukum Merek dari *Cybersquatting*	Kejahatan Nama Domain yang Berkaitan dengan Merek Ditinjau Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	Kebijakan Integral Hukum Pidana dengan *Techno Prevention* dalam Upaya Pencegahan Kejahatan *Cyberbullying*
Rumusan Masalah	1. Bagaimana bentuk perlindungan	1. Pengaturan nama domain dalam	1. Apakah dalam mencegah

	hukum terhadap merek dari tindakan *cybersquatting* di Indonesia dibandingkan perlindungan hukum terhada merek darin tindakan *cybersquatting* menurut *Anti-Cybersquatting Consumer Protection Act 1999 (ACPA* dan *Uniform Dispute Resolution Policy (UDRP)?* 2. Bagaimana peranan PANDI dalam memberikan perlindungan hukum terhadap merek dari *cybersquatting* di Indonesia?	Undang-undang Informasi dan Transaksi Elektronik. 2. Karakteristik kejahatan nama domain yang berkaitan dengan Merek.	kejahatan *cyberbullying* akan dapat dicapai dengan menggunakan hukum pidana? 2. Bagaimana formulasi kebijkan integral hukum pidana dengan menggunakan sarana *techno prevention* sebagai upaya pencegahan kejahatan *cyberbullying* di masa yang akan datang?
Tipe Penelitian	Yuridis Normatif	Hukum Normatif	Yuridis Normatif

Kesimpulan	1. Penelitian ini menjelaskan bahwa bentuk perlindungan hukum merek terhadap kejahatan *cybersquatting* di Indonesia hingga saat ini masih belum diatur secara tegas dalam peraturan perundang-undangan di Indonesia, baik dalam Undang-undang Nomor 15 Tahun 2001 tentang Merek, Kitab Undang-undang Hukum Pidana (KUHP), dan Undang-undang Nomor 8 Tahun 1999 tentang perlindungan Konsumen. Sedangkan di Amerika Serikat	1. Indonesia telah memiliki Undang-Undang ITE yang mengatur tentang nama domain dalam ketentuan umum dan pada ketentuan tertentu di bab VI, tetapi pengaturan tentang kejahatan nama domain tidan diatur dalam UU ITE tersebut sebagaimana sudah diamanatkan dalam naskah akademik RUU ITE yang telah mencantumkan norma nama domain beserta sanksi pidana. Ketiadaan pengaturan norma nama domain dalam UU ITE ini menimbulkan permasalahan dalam pendaftaran nama domain (*Regostrant*) yang dengan sengaja mendaftarkan nama	1. Kebijakan penanggulangan *cyberbullying* dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan). Dilihat dari sudut *criminal policy*, upaya penanggulangan tindak *cyberbullying* tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana, tetapi harus ditempuh juga dengan pendekatan integral serta

	perbuatan *cybersquatting* secara jelas dan tegas diatur dalam aturan hukum positif yang tertuang dalam 15 USC Sec. 1125 dan 1129 *Anti-cybersquatting Consumer Protection* menurut *Uniform Dispute Resolution Policy (UDRP)* adalah melindungi pendaftaran nama domain dari itikad tidak baik. 2. Dalam upaya untuk meningkatkan perlindungan terhadap merek dari tindakan *cybersquatting*, di Indonesia telah dilakukan oleh pemerintah melalui	domain beretikad tidak baik dengan melanggar persyaratan nama domain, pendekatan hukum pidana akan sulit diterapkan berkaitan kejahatan nama domain tersebut dan menjadi salah satu kelemahan dalam UU ITE 2. Karakteristik kejahatan pada nama domain yang berkaitan dengan merek merupakan nama domain yang didaftarkan memiliki persamaan pada pokoknya dengan merek terkenal milik pihak lain, tindakan pelakunya dengan cara memanfaatkan reputasi atas nama-nama yang sudah terkenal atau telah	dengan pendekatan teknologi. Selain itu diperlukan pula pendekatan budaya, moral, dan bahkan pendekatan global. 2. Hukum pidana memiliki kemampuan yang terbatas dalam upaya penanggulangan kejahatan yang begitu beragam dan kompleks khususnya terhadap tindakan *cyberbullying*. Oleh karena itu diperlukan adanya pendekatan *non penal*. Dilihat dari sudut

	pendelegasian wewenangnya kepada PANDI (Pengelola Nama Domain Indonesia. Peraturan PANDI mengenai nama domain berdasarkan Pasal 23 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta memberikan persyaratan untuk membuat nama domain dengan mencamtumkan pedoman pemberian nama domain dengan syarat yaitu, penamaan suatu domain perlu memenuhi ketentuan dan persyaratan nam Merek/ nama	bernila komersial sebelumnya sebagai nama domain untuk alamat bagi situs yang dikelolanya dengan tujusn untuk mendapat keuntungan dengan menjual kembali nama domain tersebut kepada pihak lain yang memerlukannya dengan harga yang lebih tinggi dari biaya pendaftarannya *(cybersquatting).*	politik kriminal, kebijakan paling strategis adalah melalui sarana *"non penal"* karena lebih bersifat preventif. Pendekatan integral antara *penal policy* dan *non penal policy* dalam penanggulangan kejahatan harus dilakukan karena pendekatan penerapan hukum pidana semata mempunyai berbagai keterbatasan.

	tanda dagang/ nama hak cipta/ HKI lainnya adalah nama domain terkait merek/ tanda dagang/ hak cipta/ HKI lainnya dari registrant/ badan usaha/ instansi/ organisasi yang didukung atau dibuktikan dengan sertifikat merek/ tanda dagang/ hak cipta/ HKI lainnya. Ketentuan tersebut membuka peluang bagi undang-undang merek di Indonesia untuk dilakukan sinkronisasi dengan peraturan yang dibuat oleh PANDI mengenai keberadaan merek dalam dunia maya.		

Namun pada tesis ini dengan judul **"Kebijakan Formulasi Pertanggungjawaban Pidana Terhadap Pelaku Kejahatan *Cybersquatting*"** dijamin keasliannya serta pembahasan dan kesimpulan dalam tesis ini akan membahas dari sudut pandang yang berbeda dengan rumusan masalah yang diangkat yaitu dapat tidaknya sistem pertanggungjawaban pidana dalam Undang-undang Informasi dan Transaksi Elektronik diterapkan dalam kasus *cybersquatting* dan kebijakan formulasi yang ideal dalam pertanggungjawaban terhadap pelaku kejahatan *cybersquatting*, hal inilah yang membedakan dengan penelitian terdahulu sehingga memberikan unsur kebaharuan dalam pertanggungjawaban terhadap pelaku kejahatan *cybersquatting*.

1.6 Metode Penelitian

Dalam suatu penulisan harus mempergunakan metode penulisan yang tepat karena hal tersebut sangat diperlukan dan merupakan pedoman dalam rangka mengadakan analisis terhadap data hasil penelitian. Ciri dari karya ilmiah di bidang hukum adalah mengandung kesesuaian dan mengandung kebenaran yang dapat dipertanggungjawabkan.[13] Mengadakan suatu penelitian ilmiah mutlak menggunakan metode, karena dengan metode tersebut berarti penyelidikan yang berlangsung menurut suatu rencana tertentu, artinya peneliti tidak bekerja secara acak-acakan melainkan setiap langkah yang diambil harus jelas serta ada

[13] Ronny Hanitijo Soemitro, *Metode Penelitian Hukum dan Jurimetri* (Jakarta: Rinneka Cipta, 1988). Hlm.10

pembatasan-pembatasan tertentu untuk menghindari jalan yang menyesatkan dan tidak terkendalikan.[14]

1.6.1 Tipe Penelitian

Pembahasan tesis ini menggunakan penelitian hukum normatif, artinya permasalahan yang diangkat, dibahas dan diuraikan dalam penelitian ini difokuskan dengan menerapkan kaidah-kaidah atau norma-norma dalam hukum positif. Tipe penelitian yuridis normatif dilakukan dengan mengkaji berbagai macam aturan hukum yang bersifat formal seperti Undang-undang, literatur-literatur yang bersifat konsep teoritis yang kemudian dihubungkan dengan permasalahan yang menjadi pokok pembahasan.[15]

1.6.2 Pendekatan Masalah

Pendekatan masalah dalam penyusunan tesis ini, yaitu:

1. Pendekatan perundang-undangan (*Statute Approach*), dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani. Isu hukum yang ditangani dalam penelitian ini mengenai pertanggungjawaban terhadap pelaku kejahatan *cybersquatting.* Hasil dari telaah tersebut merupakan suatu argumen untuk memecahkan isu yang dihadapi.[16] Pendekatan perundang-undangan dalam tesis ini menggunakan Undang-Undang Nomor 1 Tahun

[14] Johnny Ibrahim, *Teori dan Metodelogi Penelitian Hukum Normatif*, 2d ed (Malang: Banyumedia Publishing, 2006). Hlm. 294

[15] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Media Group, 2013). Hlm.194

[16] Peter Mahmud Marzuki, *Penelitian Hukum*, 9th ed (Jakarta: Prenadamedia Group, 2014). Hlm. 133

1946 tentang Peraturan Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Pendekatan Konseptual (*Conceptual Approach*), metode pendekatan merujuk pada prinsip-prinsip hukum, yang dapat diketemukan dalam pandangan-pandangan sarjana ataupun doktrin-doktrin hukum. dengan mempelajari pandangan-pandangan dan doktrin-doktrin di dalam ilmu hukum, peneliti akan menemukan ide-ide yang melahirkan pengertian-pengertian hukum, konsep-konsep hukum dan asas-asas hukum yang relewan dengan isu yang dihadapi.[17] Secara khusus, pembahasan mengenai konsep-konsep yang akan digunakan dalam tesis ini adalah mengenai konsep *cybersquatting*, konsep kebijakan hukum pidana, konsep kebijakan kriminalisasi, konsep pertanggungjawaban pidana, teori kesalahan, teori anomie, dan asas legalitas.

3. Pendekatan Perbandingan (*Comparative Approach*), pendekatan ini dilakukan dengan membandingkan undang-undang suatu negara dengan undang-undang dari satu atau lebih negara lain mengenai hal yang sama. Dapat juga yang diperbandingkan di samping undang-undang juga putusan pengadilan di beberapa negara untuk kasus yang sama.[18] Kegunaan pendekatan ini adalah untuk memeperoleh persamaan dan perbedaan di antara undang-undang tersebut. Hal ini untuk menjawab mengenai isu

[17] *Ibid*. Hlm. 135-136
[18] *Ibid*. Hlm.135

antara ketentuan undang-undang dengan filosofi yang melahirkan undang-undang itu. Dengan melakukan perbandingan tersebut, peneliti akan memperoleh gambaran mengenai konsistensi antara filosofi dan undang-undang di antara negara-negara tersebut. Hal yang sama juga dapat dilakukan dengan membandingkan putusan pengadilan antara suatu negara dengan negara lain untuk kasus serupa.[19] Penelitian dalam tesis ini menggunakan negara Amerika Serikat dan India sebagai perbandingan dalam hal pengaturan mengenai kriminalisasi kejahatan *cybersquatting* dan pengaturan mengenai pertanggungjawaban pelaku kejahatan *cybersquatting*. Penggunaan negara tersebut karena negara tersebut telah mengatur dan mengkriminalisasi mengenai kejahatan *cybersquatting*.

4. Pendekatan Historis *(Hystorical Approach)*. Pendekatan ini dilakukan dengan menelaah latar belakang apa yang dipelajari dan perkembangan apa pengaturan mengenai isu yang dihadapi.[20] Pendekatan historis diperlukan jika memang peneliti menganggap bahwa pengungkapan filosofis dan pola pikir ketika sesuatu yang dipelajari itu dilahirkan memang mempunyai relevansi dengan masa kini.[21] Pada penelitian tesis ini, peneliti menggunakan historis lahirnya Undang-undang ITE sehingga memerlukan naskah akademik dan risalah-risalah persidangan lahirnya Undang-Undang ITE.

---

[19] *Ibid.*
[20] *Ibid.* Hlm.134
[21] *Ibid.*

1.6.3 Sumber Bahan Hukum

Bahan hukum adalah sarana dalam penelitian hukum untuk memecahkan isu hukum dan sekaligus memberikan preskripsi mengenai apa yang seyogyanya diperlukan dalam penelitian hukum.[22] Sumber-sumber penelitian hukum dapat dibedakan menjadi sumber-sumber penelitian yang berupa bahan-bahan hukum primer dan bahan-bahan hukum sekunder.[23]

1) Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum uang bersifat autoritatif, artinya mempunyai otoritas. Bahan-bahan hukum primer terdiri dari perundang-undangan, catatan-catatan resmi atau risalah dalam pembuatan perundang-undangan dan putusan-putusan hakim.[24] Bahan hukum primer dalam penulisan tesis ini, meliputi:

1. Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Kitab Undang-Undang Hukum Pidana;
2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251;

Selain itu digunakan juga beberapa ketentuan peraturan perundang-undangan atau peraturan lainnya yang berkaitan dengan permasalahan yang dikaji. Bahan hukum primer tersebut kemudian dianalisis,

---

[22] *Ibid*. Hlm.181
[23] *Ibid*.
[24] *Ibid*.

dikembangkan, dibandingkan, dan diuji untuk memperoleh kebenaran pengetahuan secara teoritis dan ilmiah. Keseluruhan itu kemudian dihubungkan dan digunakan untuk mengembangkan jawaban dalam pokok permasalahan dalam tesi ini.

2) Bahan Hukum Sekunder

Sumber bahan hukum sekunder adalah bahan-bahan hukum yang erat kaitannya dengan bahan hukum primer dan dapat membantu untuk menganalisis dan memahami bahan hukum primer yang telah ada. Bahan hukum sekunder juga memberikan penjelasan mengenai bahan hukum primer seperti misalnya hasil karya tulis ilmiah para sarjana dan para ahli yang berupa literatur sehingga dapat mendukung, membantu dan melengkapi dalam membahas masalah-masalah yang timbul dalam rangka penyusunan tesis ini. Selain itu, sumber bahan hukum sekunder diperoleh dari buku-buku, artikel hukum, jurnal hukum, karya tulis ilmiah, serta data-data penunjang lain yang berkaitan dengan masalah penyusunan tesis ini.

1.6.4 Metode Pengumpulan Bahan Hukum

Pengumpulan bahan hukum pada tesis ini ialah dengan mengumpulkan bahan-bahan studi yang terkait dengan isu hukum. Penulis Mempelajari buku-buku hukum, undang-undang yang terkait dengan isu hukum, artikel dan jurnal-jurnal hukum yang terkait dengan isu hukum yang penulis angkat.

1.6.5 Analisis Bahan Hukum

Analisa bahan penelitian dalam tesis ini menggunakan analisis normatif kualitatif, yaitu cara untuk memperoleh gambaran singkat suatu masalah yang tidak didasarkan atas angka-angka statistik melainkan didasarkan atas suatu peraturan perundang-undangan yang berlaku dan berkaitan dengan permasalahan yang dibahas. Selanjutnya ditarik kesimpulan dengan menggunakan metode deduktif yaitu menyimpulkan pembahasan dari hal-hal yang bersifat umum menuju ke hal-hal yang bersifat khusus.

Hal tersebut dapat diartikan sebagai suatu pembahasan yang dimulai dari permasalahan yang bersifat umum menuju permasalahan yang bersifat khusus. Sebagai cara untuk mensrik kesimpulan dari hasil penelitian yang sudah terkumpul dipergunakan metode analisa bahan hukum deduktif, yaitu suatu metode penelitian berdasarkan konsep atau teori yang bersifat umum diaplikasikan untuk menjelaskan tentang seperangkat data dengan seperangkat data yang lainnya dengan sistematis berdasarkan kumpulan bahan hukum yang diperoleh, ditambahkan pendapat para sarjana yang memupunyai hubungan dengan bahan kajian komparatif. Langkah-langkah selanjutnya yang dipergunakan dalam melakukan suatu penelitian hukum, yaitu:[25]

a) Mengidentifikasi fakta hukum dan mengeliminir hal-hal yang tidak relevan untuk menetapkan isu hukum yang hendak dicapai;
b) Pengumpulan bahan-bahan hukum dan sekiranya dipandang mempunyai relevansi juga bahan-bahan non-hukum;

[25] *Ibid*. Hlm.214-251

c) Melakukan telaah atas isu hukum yang diajukan berdasarkan bahan-bahan yang telah dikumpulkan;
d) Menarik kesimpulan dalam bentuk argumentasi yang menjawab isu hukum;
e) Memberikan preskripsi berdasarkan argumentasi yang telah dibangun di dalam kesimpulan.

Langkah-langkah ini sesuai dengan karakter ilmu hukum sebagai ilmu yang preskriptif dan terapan. Sebagai ilmu yang bersifat preskriptif, ilmu hukum mempelajari tujuan hukum, nilai-nilai keadilan, validitas aturan hukum, konsep-konsep hukum dan norma-norma hukum. sebagai ilmu terapan, ilmu hukum menerapkan standar prosedur, ketentuan-ketentuan, rambu-rambu dalam melaksanakan aturan hukum. oleh karena itu, langkah-langkah tersebut dapat diterapkan baik terhadap penelitian untuk kebutuhan praktis meupun yang untuk kajian akademis.

BAB 2

TINJAUAN PUSTAKA

2.1 Tinjauan Umum tentang *Cybercrime*

2.1.1 Konsep *Cybercrime*

Kejahatan berbasis teknologi telematika dalam berbagai sumber sering disebut dengan istilah: Penyalahgunaan Komputer atau Kejahatan Komputer (*Computer Crime; Computer Related Crime; Computer Assisted Crime*), Kejahatan Mayantara (*Cyber Crime*), Kejahatan Internet (*Internet Crime*), Tindak Pidana Teknologi Informatika dan berbagai istilah lainnya.[26] Menurut Barda Nawawi Arief sebagaimana yang dikutip oleh widodo, pengertian *Computer Related Crime* sama dengan *Cybercrime*.[27]

Cybercrime merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan konvensional yang menggunakan atau dengan bantuan peralatan komputer.[28] Draft Virginia Computers Crime Act menyatakan bahwa computer adalah *" an electronic, magnetic, optical, electrochemical, or other hight speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communication facility directly related to or operating in conjunction with such device, but such term doesn't includean*

[26] Al Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika*, 1st ed (Yogyakarta: Atma Jaya Yogyakarta, 2010). Hlm.1

[27] widodo, *Sistem Pemidanaan dalam Cyber Crime (alternatif ancaman pidana, kerja sosial dan pidana pengawasan bagi pelaku cyber crime)*, 1st ed (Yogyakarta: Laksbang Mediatama, 2009). Hlm.23

[28] Widodo, *Hukum Pidana di Bidang Teknologi Informasi. Cyberrime Law: Telaah Teoritik dan Bedah Kasus,, Op.Cit*. Hlm.12

authomated typerwriter or type-setter, a portable hand-held calculator, or other similar device".[29] Dalam Virginia Computers Crime Act yang diterjemahkan oleh Widodo, komputer adalah peralatan elektronik, magnetik, optikal, elektrokimia, atau alat pengolah data berkecepatan tinggi yang dapat melakukan penalaran, atau fungsi penyimpanan, yang meliputi fasilitas penyimpanan atau fasilitas komunikasi yang secara langsung berhubungan dengan pengoperasian peralatan secara terpadu, tetapi istilah tersebut tidak meliputi mesin ketik atau mesin ketik elektronik, kalkulator jinjing, atau alat serupa lainnya.[30]

Dalam beberapa kepustakaan, *Cybercrime* sering diidentikkan sebagai *Computer Crime*. Menurut the U.S. department of Justice, *Computer Crime* sebagai: *"Any ilegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution"*.[31] Pendapat lain juga dikemukakan oleh *Organization for Economic Cooperation Development (OECD)* yang menggunakan istilah *computer related crime* yang berarti: *"Any illegal, unethical or unauthorized behavior involvinng automatic data processing and/or transmission data"*.[32]

Menurut Ari Juliano Gema dalam Maskun, menyatakan bahwa, *cybercrime* sebenarnya bukan hanya menggunakan kecanggihan teknologi komputer, akan tetapi juga melibatkan teknologi telekomunikasi di dalam

---

[29] widodo, *Sistem Pemidanaan dalam Cyber Crime (alternatif ancaman pidana, kerja sosial dan pidana pengawasan bagi pelaku cyber crime.)Op.Cit*. Hlm.25

[30] *Ibid*.

[31] Maskun, *Kejahatan Siber (Cyber Crime)*, 1st ed (Jakarta: Kencana, Prenada Media Group, 2013). Hlm.47

[32] *Ibid*.

pengoperasiannya.[33] Hal ini dapat dilihat pada pandangan Indra Safitri yang mengemukakan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah 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 disampikan dan diakses oleh pelanggan internet.[34]

Terminologi *cybercrime* sebenarnya hendak menunjukkan bahwa kejahatan tersebut berada dalam ranah *cyberspace*.[35] Beragam istilah dalam menyebut kejahatan telematika berimbas pada beragam definisi mengani apa yang disebut sebagai kejahatan telematika (*computer related crime/ cybercrime*). Ellen S Podgor dalam tulisannya yang berjudul: *"Computer Crime"* sebagaimana dikutip oleh Al Wisnubroto, menyatakan : *"A precise definition of computer crime is a problematic. This is becaise of the array of different forms and forums in which the crime appear. A single category cannot accommodate the wide divergence of conduct, perpetrators, victims, and motives found in examination computer crimes.*[36]

Susan W. Brenner, misalnya dalam tulisanya yang berjudul *"Defining Cyber Crime: A review of State and Federal Law"* seperti yang dikutip oleh Al Wisnubroto, tidak merumuskan definisi dari *crybercrime* namun langsung mendeskripsikannya dalam tiga kategori, yakni kejahatan-kejahatan ketika:[37]

---

[33] *Ibid*. Hlm.48
[34] *Ibid*.
[35] Wisnubroto, *Op. Cit* 26. Hlm.3
[36] *Ibid*. Hlm.4-5
[37] *Ibid*. Hlm.5

1. Komputer sebagai target aktivitas kejahatan *(Crimes in which the computer is he target of the criminal activity)*. Sebagai contohya adalah: menerobos sistem komputer tanpa hak/ ijin akses *(hacking)*, *hacking* yang diikuti dengan perbuatan penyalahgunaan lainnya seperti mengkopi/mengambil informasi secara illegal *(cracking)*, *hacking* yang diikuti dengan perbuatan merusak sistem komputer atau informasi yang ada di dalamnya *(sabotage)*;
2. Komputer sebagai alat/sarana perbuatan kejahatan *(crimes in which the computer is a tool used to commit the crime)*. Sebagai contoh adalah: penipuan *(fraud)*, pencurian *(theft)*, penggelapan *(embezzement)*, pemalsuan *(forgery)* dan kejahatan lainnya yang mempergunakan komputer sebagai alat atau sarananya;
3. Komputer sebagai aspek insidental dari perbuatan jahat *(crimes in which the use of the computer is an incidental aspect of the commission on the crime)*. Sebagai contohnya adalah: bisnis pengadaan narkoba ketika sistem pembukuan dan transaksinya menggunakan mempergunakan komputer untuk menulis surat ancaman/teror.

Dalam dua dokumken Konferensi Perserikatan Bangsa-Bangsa (PBB) tentang *The Prevention of Crime and The Treatment of Offenders* di Havana (Cuba) tahun 1990, dan di Wina (Austria) tahun 2000, memang terdapat dua istilah yang digunakan, yaitu *coybercrime* dan *computer related crime*.[38] Laporan

[38] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, 1st ed (Yogyakarta: Aswaja Pressindo, 2013). Hlm.6

dokumen Kongres PBB ke-10 di Wina, tanggal 19 Juli 2000 menggunakan istilah *computer related crime,* dengan pengertian 2 bentuk berikut.[39]

> *The term "computer related crime" had been developed encompas both the entirely new forms of crime that were directed at computer, networks an their users, and the more traditional from crime that were now being commited with the use or assistance of computer equipment"....*
>
> a. *Cybercrime in narrow sense Icomputer crime); any illegal behavior directed by means of electronic operations that targets the security of computer system and the data processed by them.*
> b. *Cybercrime in broader sense (computer-related crime); any illegal behavior commited by means of, or in relation to, a computer system network, includinng such crime as illegal possesion, offering or distributing information by means of computer system on network.*

Berdasarkan laporan tersebut dapat dimengerti bahwa *cybercrime* dibedakan menjadi 2 pengertian, yaitu dalam pengertian sempit dan luas. *Cybercrime* dalam arti sempit adalah perbuatan yang tidak sah yang menjadikan komputer sebagai sasaran atau target kejahatan, baik pada keamanan sistem maupun datanya.[40] Sedangkan *cybercrime* dalam arti luas merupakan keseluruhanbentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer.[41]

Dengan demikian, dapat dipahami bahwa pengertian *cybercrime* adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan, dan semua kejahatan tersebut adalah bentuk-bentuk perbuatan

---

[39] *Ibid*. Hlm.6-7
[40] *Ibid*. Hlm.7
[41] *Ibid*.

yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara materiel maupun melawan hukum secara formil.[42]

Dari pemaparan diatas mengenai konsep *cybercrime*, masih belum terjadi kesepakatan mengenai definisi dan konsep tentang *cybercrime*. Hal tersebut senada dengan yang diungkapkan oleh Agus Raharjo bahwa istilah *cybercrime* sampai saat ini belum terdapat satu kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cybercrime* dengan *computer crime.*[43]

2.1.2 Karakteristik dan Jenis *Cybercrime*

Terdapat dua pendapat mengenai kejahatan telematika sebagai kejahatan yang berteknologi tinggi. Pendapat pertama menyatakan bahwa kejahatan telematika merupakan kejahatan jenis baru yang berbeda dengan kejahatan konvensional. Pendapat yang kedua menyatakan bahwa kejahatan telematika sejatinya kejahatan konvensional dengan menggunakan teknologi canggih sebagai sarananya dan/atau sasarannya.[44]

Pendapat pertama lebih mengedepankan pada perbedaan karakteristik antara kejahatan konvensional yang berbasis sistem manual dengan kejahatan modern yang berbasis *computerized/electronic/ digitalized*.[45] Pendapat kedua, tidak mengabaikan perbedaan-perbedaan antara sistem manual dan sistem elektronik yang mempengaruhi bentuk dan sifat kejahatan ekonomi yang berbasis

---

[42] *Ibid.*

[43] Agus Raharjo, *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: Citra Aditya Bhakti, 2002). Hlm.227

[44] Wisnubroto, *Op.Cit*. Hlm.6-7

[45] *Ibid*. Hlm.7

teknologi, namun memandang bahwa perbedaan karakteristik kejahatan ekonomi berbasis teknologi tersebut hanya sebagai varian dari bentuk kejahatan konvensial, yakni: pencurian, penipuan, penggelapan, penyelundupan, dan berbagai perbuatan tidak jujur atau curang lainnya.[46] Namun demikian, baik pendapat pertama maupun pendapat kedua mengakui bahwa secara kriminologis kejahatan berbasis teknologi telematika mengarah pada jenis *white collar crime* dan *organized crime* yang memerlukan upaya penanggulan secara serius.[47]

Menurut Abdul Wahid dan M. Labib, *cybercrime* memiliki beberapa karakteristik, ialah:[48]

1. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis terjadi diruang/wilayah siber, sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya;
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang berhubungan dengan internet;
3. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
4. Pelakunya adalah orang yang menguasai penggunaan internet dan aplikasinya;
5. Perbuatan tersebut sering dilakukan secara *transnasional*.

Penjelasan di atas hanya memberikan perbedaan antara kejahatan konvensional dengan *cybercrime* dalam hal yurisdiksinya saja. Pada dasarnya,

---

[46] *Ibid*.
[47] *Ibid*.
[48] Abdul Wahid & Mohammad Labib, *Kejahatan Mayantara (cybercrime)* (Jakarta: PT. Refika Aditama, 2005). Hlm.76

kemajuan dalam bidang teknologi dan digital yang mengakibatkan munculnya *cybercrime*. Kemajuan tersebut memudahkan orang-orang untuk mendapatkan informasi dan komunikasi secara cepat. Dengan demikian, karakteristik dari *cybercrime* adalah pemanfaatan teknologi informasi (internet) untuk aktivitas kejahatan.

Cybercrime memiliki bentuk beragam yang berbeda dalam setiap negara. Secara umum, Ari Juliano Gema mengemukakan bahwa *cybercrime* dapat dikelompokkan dalam 7 bentuk, yaitu:[49]

1. *Anauthorized Access to Computer System and Service.* Kejahatan ini dilakukan dengan cara memasuki atau menyusup secara tidak sah ke dalam suatu sistem atau jaringan komputer. Tujuan dari perbuatan tersebut adalah sabotase atau pencurian data atau pemalsuan informasi penting dan rahasi. Ciri utama kejahatan ini adalah "perbuatan memasuki sistem secara tidak sah". Apakah seseorang setelah memasuki kemudian melakukan perbuatan lanjutan yang merugikan korban atau tidak, bukan merupakan unsur yang menentukan kejahatan.
2. *Illegal Contents*. Kejahatan ini dilakukan dengan jalan memasukkan data atau informasi ke dalam jaringan internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Perbuatan tersebut misalnya berupa pemuatan suatu berita bohong, fitnah, prnografi, pembocoran rahasia negara, agitasi dan

[49] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara, Op. Cit.* Hlm.163-165

propaganda untuk melawan pemerintahan yang sah. Unsur utama kejahatan ini adalah pas "isi" data yang dimasukkan ke jaringan komputer.

3. Data Forgery. Kejahatan ini dilakukan dengan acara memalsu data pada dokumen-dokumen penting yang tersimpan dalam sistem komputer sebagai *scriptless document* melalui internet. Kejahatan jenis ini biasanya ditujukan pada dokumen-dokumen perdagangan elektronik *(e-commerce)* dengan cara membuat pesan seolah-olah terjadi kesalahan pengetikan yang dapat menguntungkan pelaku, karena korban sudah terlanjur memasukkan data pribadi dan PIN kartu kredit sehingga pelaku memungkinkan menyalahgunakan data tersebut.
4. *Cyber Espionage.* Kejahatan ini dilakukan dengan jalan memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata (spionase) terhadap pihak lain dengan cara memasuki sistem jaringan komputer *(computer network system)* pihak lain. Kejahatan ini biasanya ditujukan terhadap orang atau perusahaan saingan bisnis yang dokumen atau data rahasia *(data base)* tersimpan dalam suatu sistem komputer yang tersambung ke jaringan komputer.
5. *Cyber Sabotage and Extortion.* Kejahatan jenis dilakukan dengan cara membuat gangguan, perusakan atau penghancuran terhadap data, program atau sistem jaringan komputer yang terhubung dengan internet secara tidak sah. Kejahatan ini dilakukan dengan cara menyusupkan suatu *logic bom*, virus komputer, atau suatu program tertentu, sehingga data atau program atau sistem jaringan komputer tidak dapat digunakan, tidak dapat

beroperasi sebagaimana mestinya, atau dapat beroperasi tetapi tidak sesuai dengan kehendak pelaku kejahatan. Dalam beberapa kasus, setelah kejahatan tersebut terjadi pelaku atau anggota komplotan pelaku menawarkan jasa kepada korban untuk memperbaiki data atau program atau sistem jaringan komputer yang telah disabotase, dengan meminta bayaran tertentu. Dengan demikian, pelaku (melalui komplotannya) memeproleh keuntungan secara ekonomi.

6. *Offense againt Intellectual Property*. Kejahatan jenis ini ditujukan terhadap Hak atas Kekayaan Intelektual (HaKI) yang dimiliki oleh pihak lain di internet. Sebagai contoh adalah penjiplakan tampilan *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang merupakan rahasia dagang pihak lain.
7. *Infringment of Privacy*. Kejahatan ini ditujukan terhadap data atau informasi seseorang yang bersifat individual dan rahasia *(privacy)* secara melawan hukum. kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*. Jika data tersebut diketahui oleh orang lain, dapat merugikan pemilik informasi baik secara materiil maupun immateriil, misalnya nomor kartu kredit, *Personal Identification Number (PIN)* di *Authorized Teller Machine (ATM)*, catatan-catatan pribady *(diary)*, cacat tubuh atau penyakit-penyait tersembunyi.

Jonathan Rosenoer dalam Widodo, menjelaskan tentang bentuk-bentuk *cybercrime* sebagai berikut:[50]

1. *Copyright, include exclusive right, subject matter of copyright, formalities, infringement, source of risk, word wide web sites, hypertext link, graphical element, e-mail, criminal liability, fair use, first amandment, and softwere rental.*
2. *Trademark*
3. *Defamation*
4. *Privacy, include common law privacy, constitutional law, anonymity, and technology expanding privacy right.*
5. *Duty of care*
    a. *Negligence*
    b. *Negligent misstatement*
    c. *Equipment malfunctions*
    d. *Economic loss may not be recoverable*
    e. *Contractural limitations of liability*
6. *Criminal liability,* meliputi*: computer fraud and abuse act, wire fraud, electronic communication privacy act, extortion and threats, expose, sexual exploitation of children, obscence and indecent telephone call, copyright stalking.*
7. *Pricedural issue, include jurisdiction, venue and conflict of law.*
8. *Electronic contract and digital signature, include electronic agreement enforceable, public key encryption and digitalsignature.*

Cybercrime meliputi pelanggara hak kekayaan intelektual, fitnah atau pencemaran nama baik, pelanggaran terhadap kebebasan pribadi *(privacy)*, ancaman, dan pemerasan, eksploitasi seksual anak-anak dan kecabulan, perusakan sistem komputer, pembobolan kode akses, dan pemalsuan tanda tangan digital. Semua perbuatan tersebut dapat dipertanggungjawabkan secara pidana sesuai dengan yurisdiksinya.[51] *Cybercrime* juga dapat berbentuk pemalsuan data, penyebaran virus komputer ke jaringan kumputer atau sistem komputer,

[50] *Ibid*. Hlm.165
[51] *Ibid*. Hlm.165-166

penambahan atau pengurangan sistem instruksi dalam jaringan komputer, pembulatan angka, perusakan data, dan pembocoran data rahasia.[52]

The International *Handbook on Computer crime* mengklasifikasikan *cybercrime* kedalam tiga kategori. Kategori pertama, *cybercrime* adalah kejahatan ekonomi yang terkait dengan komputer, meliputi penipuan dengan manipulasi komputer, pembajakan perangkat lunak komputer, spionase komputer, sabotase, pencurian jasa, akses tidak sah ke dalam sistem atau jaringan komputer, komputer sebagai alat untuk menyerang bisnis tradisional. Kategori kedua, adalah pelanggaran terhadap keleluasaan pribadi, yaitu penggunaan data yang tidak benar, pengumpulan data secara tidak sah, penyalahgunaan data, pelanggaran rahasia perusahaan. Sedangkan, kategori ketiga, misalnya melakukan penyerangan terhadap negara dan kepentingan politk, dan penyerangan terhadap kebebasan pribadi orang per orang.[53]

Selaian penggolongan *cybercrime* yang telah disebutkan di atas, Donn Parker mengklasifikasikan bentuk *cybercrime* menjadi empat golongan, yaitu:[54]

1. Komputer sebagai objek

   Dalam kategori ini, bentuk-bentuk *cybercrime* termasuk kasus-kasus perusakan terhadap komputer, data atau program yang terdapat di dalamnya atau perusahaan terhadap sarana-sarana komputer seperti *Air Conditioning* (AC) dan peralatan listrik yang menunjang pengoperasian komputer.

2. Komputer sebagai subjek

[52] *Ibid*.
[53] *Ibid*. Hlm.167
[54] *Ibid*. Hlm.168

Komputer dapat pula menimbulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya oencurian, penipuan, dan pemalsuan yang menanyangkut harta benda dalam bentuk baru yang tidak dapat disentuh *(intangible)*, misalnya pulsa elektrinis dan guratan-guratan magnetis.

3. Komputer sebagai alat

   Komputer digunakan sebagai alat untuk melakukan kejahatan sehingga sifat peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh adalah seorang pelaku kejahatan yang mengambil warkat-warkat setoran dari suat bank dan menulis nomor rekening pelaku dengan tinta magnetis pada warkat-warkat tersebut, kemudian meletakkan kembali di tempat semula. Nasabah yang akan memasukkan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomor rekening pelaku kejahatan tersebut sebagai bukti penyetoran. Pada waktu komputer memproses warkat-warkat nasabah, komputer secara otomatis akan mengredit sejumlah uang pada rekening pelaku kejahatan. Selain itu, pelaku kejahatan menarik uang dengan cek dari rekeningnya sebelum para nasabah yang menyetor mengajukan komplain ke bank.

4. Komputer sebagai simbol

   Suatu komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman. Dalam kategori ini termasuk penipuan melalui “biro jodoh” yang menyatakan bahwa biro jodoh tersebut memakai komputer untuk membantu si korban mencari jodoh, akan tetapi ternyata biro jodoh tersebut tersebut sama sekali tidak memakai komputer untuk keperluan tersebut.

Secara yuridis (internasional) pada akhir tahun 2011, *Convention on Cybercrime* menentukan bentuk-bentuk *cybercrime*, yaitu:[55]

1. Akses tidak sah terhadao sistem komputer;
2. Sengaja dan tanpa hak mendengar atau menangkap atau menyadap secara diam-diam pengiriman transmisi dalam dan melalui sistem komputer dengan menggunakan peralatan teknis tertentu;
3. Tanpa hak melakukan perubahan, perusakan atau penghapusan data; mengganggu data; mengganggu sistem komputer, dan penyalahgunaan perlengkapan perangkat lunak komputer;
4. Pemalsuan yang berhubungan denngan komputer yaitu dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data otentik menjadi tidak ptentik dengan maksud untuk digunakan sebagai data otentik;
5. Penipuan yang berhubungan dengan komputer, yaitu melakukan dengan sengaja dan tanpa hak yang menyebabkan hilangnya barang atau harta kekayaan orang lain dengan cara memasukkan, mengubah, menghaus data komputer, atau dengan mengganggu fungsi komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi diri sendiri atau orang lain;
6. Tindak pidana yang berhubungan dengan pronografi anak, meliputi perbuatan memproduksi dengan tujuan mendistribusikan melalui sistem komputer, menawarkan melalui sistem komputer, mendistribusikan atau mengirim melalui sistem komputer, memperoleh melalui sistem komputer,

[55] *Ibid*. Hlm.171-172

memiliki dalam sistem komputer atau di dalam media penyimpanan data komputer lainnya'

7. Pelanggaran yang berhubungan dengan hak cipta dan hak-hak lain yang terkait.

Berdasarkan uraian tentang bentuk-bentuk *cybercrime* di atas dapat disimpulkan bahaw sampai saat ini para ahli hukum belum menyepakati tentang bentuk-bentuk dari *cybercrime*. Tetapi secara umum bentuk *cybercrime* dapat dikategorikan menjadi dua, yaitu komputer sebagai alat melakukan kejahatan, dan sebagai sarana kejahatan.[56]

2.1.3 Pengaturan *Cybercrime*

Jauh sebelum Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diundangkan, di Indonesia untuk menjangkau *cybercrime* para penegak hukum menggunakan pasal-pasal KUHP dan peraturan-peraturan diluar KUHP untuk mengadili pelaku *cybercrime*. Namun, setelah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diundangkan, Indonesia telah mempunyai undang-undang khusus yang mengatur tentang kejahatan-kejahatan yang terjadi di dunia maya *(cybercrime)*, sehingga tidak lagi menggunakan KUHP untuk mengadili para pelaku *cybercrime*.

Ketentuan dalam KUHP yang digunakan untuk menangani *cybercrime* adalah ketentuan tentang pemalsuan (Pasal 263-276), pencurian (Pasal 362-367),

[56] *Ibid*. Hlm.172

penipuan (Pasal378-395), perusakan barang (Pasal 407-412)[57] dan peraturan perundang-undangan lain di luar KUHP.

Setelah Undang-undang Informasi dan Transaksi Elektronik, Indonesia mengklasifikasikan *cybercrime* dalam beberapa kategori sebagai berikut:[58]

1. Akses Tidak Sah *(Illegal Access)*

Perbuatan yang memenuhi unsur tindak pidana akses secara tidak sah terhadap komputer dan/atau sistem elektronik milik orang lain diatur dalam Pasal 30 Undang-undang Informasi dan Transaksi Elektronik.

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengsn tujusn 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 dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

2. Penyadapan atau Interepsi Tidah Sah *(Intercepting)*

[57]Widodo, *Hukum Pidana di Bidang Teknologi Informasi. Cybercrime Law: Telaah Teoritik dan Bedah Kasus. Op. Cit*. Hlm.32

[58] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara. Op. Cit*. Hlm.107-113

Tindak pidana intersepsi diatur dalam Pasal 31 Undang-undang Informasi dan Transaksi Elektronik.

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun meupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

(3) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang.

Mahkamah Konstitusi (MK) melalui Putusan Nomor.5/PUU-VIII/2010 telah membatalkan ketentuan Pasal 31 ayat (4) Undang-undang Informasi Transaksi dan Elektronik yang berisi tata cara penyadapan yang hanya diatur oleh Peraturan Pemerintah. Karena itu, ketentuan pasal tersebut tidak berlaku. Hal ji

dapat dipahami karena pembatasan melalui penyadapan harus diatur dengan undang-undang agar terhindar dari penyalahgunaan wewenang yang melanggar HAM. Pengaturan penyadapan di Indonesia hanya dapat dilakukan dengan Undang-undang, karena menyangkut pembatasan HAM yang mendasar, sebagaimana tersirat diatur Pasal 28 J ayat (2) UUD 1945.[59]

3. Gangguan Terhadap Data Komputer *(Data Interference)*

Tindak pidana perubahan data dan gangguan terhadap data komputer diatur dalam Pasal 32 Undang-undang Informasi dan Transaksi Elektronik, yaitu:

(1) 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.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik prang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

4. Gangguan Terhadap Sistem Komputer *(Sistem Interference)*

Tindak pidana berupa gangguan sistem diatur dalam Pasal 33 Undang-undang Informasi dan Transaksi Elektronik berikut. Setiap orang dengan sengaja

[59] *Ibid*. Hlm.109

dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggnya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

5. Penyalahgunaan Perangkat Lunak Komputer *(Misuse Of Device)*

Tindak pidana berupa penyalahgunaan perangkat komputer diatur dalam Pasal 34 Undang-undang Informasi dan Transaksi Elektronik, yaitu:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
   a. Perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
   b. Sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

(2) Tidakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian sistem elektronik, untuk perlindungan sistem elektronik itu sendiri secara sah dan tidak melawan hukum.

6. Pemalsuan Melalui Komputer *(Computer-Related Forgery)*

Pemalsuan melalui komputer diatur dala Pasal 35 Undang-undang Informasi dan Transaksi Elektronik berikut, setiap orang dengan sengaja dan

tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

7. Pornografi Melalui Komputer *(Pornography)*

Perbuatan pidana pornografi diatur dalam Pasal 27 Undang-undang Informasi dan Transaksi Elektronik sebagai berikut.

(1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau dokumen elektronik yang meiliki muatan yang melanggar kesusilaan.

Berdasarkan uarian di atas dapat dipahami bahwa kriminalisasi terhadap tindak pidana pornografi di internet bukan hanya terhadap pornografi anak tetapi juga pornografi dewasa.[60]

8. Kejahatan "Tradisional" yang Menggunakan Komputer

Perbuatan pidana tradisonal juga diatur dalamPasal 27 ayat (2), (3), dan (4) Undang-undang Informasi dan Transaksi Elektronik sebagai berikut.

(2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian.

(3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik

[60] *Ibid*. Hlm.112

dan/atau dokumen elektronik yang memiliki muatam pemghinaan dan/atau pencemaran nama baik.

(4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentrasmisikan dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Selain itu, tindak pidana berupa penyebaran berita bohong melalui internet diatur dalam Pasal 28 Undang-undang Informasi dan Transaksi Elektronik sebagai berikut.[61]

(1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

(2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).

Tindak pidana pengancaman melalui internet kepada seseorang diatur dalam Pasal 29 Undang-undang Informasi dan Transaksi Elektronik, yaitu setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menaku-nakuti yang ditujukan secara pribadi.[62]

[61] *Ibid*. Hlm.113
[62] *Ibid*.

2.2 Konsep *Cybersquatting*

Cybersquatting merupakan salah satu kejahatan dalam dunia siber *(cybercrime)* yang berhubungan dengan nama domain. Secara sederhana, nama domain dapat dikatakan seperti nomor telepon dan alamat rumah seseorang. Pada awalnya, nama domain *(domain name)* digunakan hanya untuk mengidentifikasi komputer. Penggunaannya kemudian menjadi lebih intensif dan nama domain menjadi bagian dari identitas seseorang (seperti misalnya alamat email atau alamat situs web).[63] Penggunaan nama domain sejatinya hanya untuk pemakain internet. Hal tersebut sesuai dengan yang dikemukan oleh Andrew R. Basile dalam jurnal Internasional. Beliau menyatakan bahwa:[64]

> *The internet is a network of computers interconnected for electronic communication. Every computer connected to the internet is assigned a numeric address, which the other computers on the network use to route messages to that computer. A typical numeric internet address is 200.98.102.23. these addresses are difficult for humans to remeber, so the internet authorities also assign alphanumeric addresses, or domain name. Example of domain name include "whitehouse.gov" or "microsoft.com".* (*Terjemahan Penulis: Internet adalah jaringan komputer yang saling terhubung untuk komunikasi elektronik. Setiap komputer yang terhubung ke internet diberi alamat numerik, yang digunakan komputer lain untuk digunakan dalam rute pesan ke komputer tersebut. Alamat internet numerik yang khas adalah 200.98.102.23. alamat ini sulit bagi manusia untuk mengingat, jadi pihak berwenang internet juga menetapkan alamat alfanumerik, atau nama domain. Contoh nama domain termasuk "whitehouse.gov" atau "microsoft.com").

Penggunaan nama domain yang begitu pesat menyebabkan nama domain memiliki nilai bisnis yang menggiurkan, sehingga mulai terjadi jual beli nama

[63] Tampubolon, *Op. Cit*. Hlm.7

[64] Andrew R Basile, Jr, "Risghts to Domain Names" (1996) Online Law SPAs Leg Guide Doing Bus Internet 227.

domain dan bahkan saling membajak nama domain.[65] Aktivitas yang berhubungan dengan jual beli, bajak, mendaftarkan nama orang dan sejenisnya disebut sebagai *cybersquatting*.[66]

Black Law Dictinionary memberikan penjelasan mengenai *cybersquatting*, yaitu:[67]

> *Cybersquatting: the act of reserving a domain name on the internet, esp. a name that would be associated with a company's trademark, and then seeking to profit by selling or licensing the name to the company that has an interest in being identified with it. The practice was banned by federal law in 1999.* (*Terjemahan penulis. *Cybersquatting:* tindakan memesan nama domain di internet, esp. nama yang akan dikaitkan dengan merek dagang perusahaan, dan kemudian mencari keuntungan dengan menjual atau memberi lisensi nama tersebut kepada perusahaan yang memiliki kepentingan untuk diidentifikasi dengannya. Praktek tersebut dilarang oleh undang-undang federal pada tahun 1999).

International Journal of Law and Information Technology juga menulis tengang *cybersquatting*, yaitu:[68]

> *Cybersquatting is a particular type of domain name dispute which occurs when someone register a domain which is associated with a famous firm with the sole intention of selling it on to them at a higher price* (*Terjemahan Penulis. *Cybersquatting* adalah salah satu jenis kejahatan yang berupa sengketa nama domain yang terjadi pada saat seseorang mendaftarkan nama domain tersebut yang dikaitkan dengan nama perusahaan terkenal dengan tujuan menjual nama domain tersebut kepada perusahaan yang bersangkutan dengan harga yang lebih tinggi)

International Jurnal of Law and Infromation yang berjudul *"Cybersquatting: Prevention Better Than Cure?"* menyatakan bahwa *Of all of the*

---

[65] Tampubolon, *Op. Cit*. Hlm.9
[66] *Ibid*.
[67] Bryan A Garner, *Black's Law Dictionary*, 10th ed (United States of Amerika: Thomson Reuters, 2014). Hlm.470
[68] Moore, *Loc. Cit.*

cybercrimes, cybersquatting as a phenomenon, was the one that received the most attention as it rapidly increased as quickly as the commercialisation of the internet in the mid 1990's, as many entrepreneurial types quickly realised the money to be made from forcing big brands into buying such coveted sites as wallstrees.com which was bought for $70 and sold for $1 million (*Terjemahan Penulis. Dari semua *cybercrimes, cybersquatting* merupakan salah satu fenomena yang telah mendapat banyak perhatian karena peningkatannya yang sangat cepat seiring perkembangan internet di pertengahan tahun 1990-an, karena banyak jenis kewiraswastaan dengan cepat menyadari bahwa uang itu harus dibuat dari memaksa besar merek membeli situs yang didambakan seperti wallstrees.com yang dibeli seharga $ 70 dan dijual seharga $ 1 juta)

Benjamin Wright and Jane K. Winn menyatakan bahwa *"The practice of registering domain names that are similar to existing trade marks but have not yet been registeres by trademark owner is referred to as "cybersquatting" and has been sharply critized by some courts"*[69] (Terjemahan Penulis. Parktek mendaftarkan nama domain yang mirip dengan merek dagang yang ada namun belum terdaftra oleh pemilik merek dagang tersebut sebagai *"cybersquatting"* dan telah dikritik dengan tajam oleh beberapa pengadilan).

Jadi, *cybersquatting* pada dasarnya adalah praktek-praktek oleh para pihak-pihak tertentu untuk mendahului mendaftarkan suatu nama domain tertentu yang terkait dengan perusahaan lain tertentu dengan tujuan memperoleh

[69] Tampubolon, *Loc. Cit*.

keuntungan besar dengan cara menjual nama domain tersebut kepada perusahaan yang berhak memiliki nama domain tersebut.[70]

Dalam hukum positif Indonesia, pengaturan mengenai kejahatan yang berkaitan dengan nama domain masih belum di atur secara jelas. Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik hanya mengatur mengenai penjelasan, prosedur, dan pengelolaan nama domain. Undang-undang ITE tidak mengatur mengenai kejahatan nama domain yang dalam hal ini *cybersquatting*.

2.3 Kebijakan Hukum Pidana

Perkembangan masyarakat di zaman modern yang begitu pesat akibat berkembangnya ilmu pengetahuan dan teknologi (Iptek), perlu diikuti dengan kebijakan di bidang hukum sebagai sarana untuk menertibkan dan melindungi masyarakat dalam mencapai kesejahteraannya.[71]

Kebijakan hukum pidana juga sering disebut dengan pembaharuan dalam bidang hukum pidana. Kata kebijakan berasal dari bahasa Inggris yaitu *Policy* yang artinya kebijakan. Kata *policy* sering dikaitkan dengan politik yang mengakibatkan pembaharuan hukum pidana sering disebut dengan politik hukum pidana atau kebijakan formulatif yang diartikan sebagai upaya untuk melakukan reorientasi dan reformasi hukum pidana yang sesuai dengan nilai-nilai sosiopolitik, sosiofilosofis, serta sosiokultural masyarakat Indonesia yang

[70] *Ibid*. Hlm.46-47

[71] Dey Ravena & Kristian, *Kebijakan Kriminal (Criminal Policy)*, 1st ed (Jakarta: Kencana, Prenada Media Group, 2017). Hlm.113

melandasi kebijakan sosial, kebijakan kriminal dan kebijakan penegakan hukum di Indonesia.[72]

Kebijakan hukum pidana, politik hukum pidana, atau pembaharuan hukum pidana, begitu juga dengan kebijakan formulatif dan kebijakan perundang-undangan, merupakan istilah yang sinonim, yang merupakan salah satu permasalahan yang di hadapi oleh bangsa. Hal ini disebabkan karena sebagian besar hukum di Indonesia merupakan penerusan dari sistem hukum sebelumnya, dengan alasan untuk mencegah kekosongan hukum *(rechtsvacuum),* ketentuan hukum penjajah tetap diberlakukan sampai diadakan yang baru sesuai dengan sistem ketatanegaraan maupun falsafah hidup bangsa Indonesia.[73]

Kebijakan hukum pidana dalam bahasa Belanda diungkapkan dengan istilah *strafrecht politiek* yang oleh Murder dinyatakannya sebagai garis kebijakan untuk menentukan:[74]

1) Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu diubah atau diperbarui?
2) Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana?
3) Bagaimana cara penyidikan, penuntukan, peradilan, dan pelaksanaan pidana harus dilaksanakan?

Kebijakan hukum pidana lebih menitikberatkan kepada usaha untuk memperbaharui hukum khususnya hukum pidana materiil. [75] pemikira Murder di atas bertolak dari pengertian sistem hukum pidana yang menyatakan bahwa tiap

[72] Barda Nawawi Arief, *Kebijakan Hukum Pidana, Perkembangan Penyusunan Konsep KUHP Baru* (Jakarta: Kencana, Prenada Media Group, 2008). Hlm.25
[73] M Ali Zaidan, *Kebijakan Kriminal*, 1st ed (Jakarta: Sinar Grafika, 2016). Hlm.124-125
[74] *Ibid*. Hlm.125
[75] *Ibid*.

masyarakat yang terorganisasi, memiliki sistem hukum pidana yang terdiri atas peraturan-peraturan hukum pidana dan sanksinya, suatu prosedur hukum pidana, serta suatu mekanisme pelaksanaan (pidana).[76]

Kebijakan hukum pidana *(penal policy)* menurut Marc Ancel, ialah suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak hanya kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada penyelenggara atau pelaksana putusan pengadilan.[77]

Dengan demikian, dilihat sebagai bagian dari politik hukum maka kebijakan hukum pidana mengandung arti, bagaimana mengusahakan atau membuat dan merumuskan suatu perundang-undangan pidana yang baik, hal tersebbut terlihat dari pengertian *"penal policy"* yang diungkapkan oleh Marc Ancel. Beliau menyatakan bahwa kebijakan hukum pidana merupakan suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik. Oleh karenanya, yang dimaksud dengan "peraturan hukum positif" *(the positive rules)* dalam definisi Marc Ancel tersebut, jelas adalah peraturan perundang-undangan hukum pidana sedangkan istilah *"penal policy"* menurut Marc Ancel adalah sama dengan istilah "kebijakan atau politik hukum pidana.[78]

[76] *Ibid.*
[77] Ravena, *Op. Cit*. Hlm.116
[78] *Ibid*. Hlm.117

Kebijakan penal *(penal policy)* meliki peranan yang sangat penting dalam hal menanggulangi kejahatan dan penegakan hukum pidana. Salah satu kesimpulan seminar kriminologi ke-3 tahun 1967 menyatakan bahwa hukum pidana hendaknya dipertahankan sebagai salah satu sarana untuk *"social defence"* dalam arti melidungi masyarakat terhadap kejahatan dengan memperbaiki atau memulihkan kembali (rehabilitasi) si-pembuat tanpa mengurangi keseimbangan kepentingan perorangan (pembuat) dan masyarakat.[79]

Upaya penal sebagaimana dikemukakan oleh Hoefnagels terletak pada penerapan *criminal policy*, khususnya pada bagian *criminal law application* atau penerapan hukum pidana, artinya suatu perkara dilakukan pengusutan mulai peneyelidikan atau penyidikan, penuntutan, sampai pemeriksaan di sidang pengadilan.[80]

Operasional kebijakan hukum dengan sarana penal terdapat beberapa tahap yang harus dilalui, yaitu:[81]

1) Tahap formulasi (kebijakan legislatif);
2) Tahap aplikasi (kebijakan yudikatif/yudisial);
3) Tahap eksekusi (kebijakan eksekutif/administratif).

Dengan adanya tahap "formulasi", maka upaya pencegahan dan penanggulangan kejahatan bukan hanya tugas aparat penegak/penerap hukum, tetapi juga tugas

[79] Muladi & Barda Nawawi Arief, *Teori-teori dan Kebijakan Hukum Pidana*, 4th ed (Bandung: PT. Alumni, 2010). Hlm.92

[80] Zaidan, *Loc. Cit*.

[81] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, 4th ed (Jakarta: Kencana, Prenada Media Group, 2014). Hlm.78-79

aparat pembuat hukum (aparat legislatif), bahkan kebijakan legislatif merupakan tahap paling strategis dari *penal policy*.[82]

2.4 Pertanggungjawaban Pidana

Pada zaman revolusi Perancis, pertanggungjawaban pidana tidak hanya diterapkan pada manusia tetapi pertanggungjawaban pidana dapat juga dikenakan pada hewan dan benda mati lainnya. Berbicara tentang pertanggungjawaban tidak lepas dari seorang filsafah hukum yaitu Roscou Pound. Rouscou Pound dalam *"An Introduction to the Philosophy of Law"*, beliau menyatakan bahwa *"I...use the simple word "liability" for the situation whereby one axact legally and other is legally subjected to the exaction"*.[83]

Konsep pertanggungjawaban Rouscou Pound bertitik tolak pada sudut pandang filosofis dan sistem hukum secara timbal balik. Dalam sudut pandang filosofis, secara sistematis Rouscou Pound menyatakan bahwa "liabilty" dapat diartikan dengan suatu kewajiban yang diterima pelaku sebagai pembalasan atas perbuatan yang dilakukan oleh pelaku dari seseorang yang dirugikan. Hal tersebut sejalan dengan semakin efektifnya perlindungan yang diberikan undang-undang kepada masyarakat akan suatu kedamaian dan ketertiban, serta adanya suatu keyakinan yang menyatakan bahwa pembalasan merupakan alat penangkal, maka kedudukan ganti rugi bergeser dari suatu hak istimewa menjadi suatu kewajiban. Ukuran ganti rugi tersebut tidak lagi hanya dari suatu nilai pembalasan yang harus

[82] *Ibid*. Hlm.79
[83] Romli Atmasasmita, *Asas-asas Perbandingan Hukum Pidana*, 1st ed (Jakarta: Yayasan LBH, 1989). Hlm.79

dibeli melainkan dari sudut penderitaan yang ditimbulkan dari perbuatan pelaku.[84] Perubahan wujud ganti rugi dengan sejumlah uang kepada ganti rugi penjatuhan hukuman merupakan awal dari adanya pertanggungjawaban.[85]

Konsep pertanggungjawaban pidana di atas sesungguhnya tidak hanya menyangkut soal hukum semata, akan tetapi juga menyangkut soal nila moral atau kesusilaan umum yang dianut oleh suatu masyarakat atau kelompok-kelompok dalam masyarakat.[86] Berbicara tentang pertanggungjawaban pidana tidak lepas dari perbuatan pidana, sebab seseorang tidak dapat di mintai pertanggungjawaban tanpa melakukan perbuatan pidana sebelumnya. Tidak adil apabila seseorang harus betanggungjawab atau suatu perbuatan pidana tetapi ia sendiri tidak melakukan perbuatan tersebut.[87]

Ajaran kesalahan merupakan konsep sentral dalam pertanggungjawaban dalam hukum pidana. Ajaran kesalahan dikenal dengan sebutan *mens rea* (bahasa latin). Doktrin *mens rea* dilandaskan pada suatu perbuatan tidak mengakibatkan orang bersalah kecuali pemikiran orang itu jahat. Berdasarkan asas tersebut terdapat 2 syarat yang harus dipenuhi untuk dapat memidana seseorang, yaitu ada perbuatan yang dilarang/perbuatan pidana *(actus rea)*, dan sikap batin tercela *(mens rea)*.[88]

Pertanggungjawaban pidana menurut Roeslan Saleh ialah diteruskannya celaan (objektif) yang terdapat dalam perbuatan pidana dan memenuhi syarat

---

[84] *Ibid*. Hlm.80
[85] *Ibid*.
[86] Hanafi Amrani & Mahrus Ali, *Sistem Pertanggungjawaban Pidana Perkembangan dan Penerapan*, 1st ed (Jakarta: PT. RajaGrafindo Persada, 2015). Hlm.17
[87] Roeslan Saleh, *Perbuatan Pidana dan Pertanggungjawaban Pidana; Dua Pengerrtian Dasar dalam Hukum Pidana*, 3d ed (Jakarta: Aksara Baru, 1983). Hlm.20-23
[88] Amrani & Ali, *Op. Cit*. Hlm.20-21

untuk dapat dipidana atas perbuatan tersebut (subjektif).[89] Berkaitan dengan celaa objektif dan celaan subjektif, Sudarto menyatakan bahwa dipidananya seseorang tidaklah cukup apabila orang itu melakukan perbuatan yang bertentangan dengan hukum atau bersifat melawan hukum, artinya meskipun perbuatan tersebut memenuhi rumusan delik namun hal tersebut masih belum memenuhi syarat penjatuhan pidana. Agar pemidanaan dapat diterapkan, syarat penjatuhan pidana harus dipenuhi terlebih dahulu yaitu, orang yang melakukan perbuatan tersebut mempunyai kesalahan (celaan subjektif).[90]

Secara terperinci, Sudarto menyatakan agar seseorang memeliki aspek pertanggungjawaban pidana harus memenuhi beberapa syarat, yaitu:[91]

1. Adanya suatu tindak pidana yang dilakukan oleh pembuat;
2. Adanya unsur kesalahan berupa kesengajaan atau kealpaan;
3. Adanya pembuat yang mampu bertanggung jawab;
4. Tidak ada alasan pemaaf.

Pada dasarnya steiap subjek hukum baik orang perseorangan, badan hukum, dan korporasi yang terbukti melakukan suatu tindak pidana harus mempertanggungjawabkan perbuatannya tersebut. Unsur dari pertanggungjawaban pidana menurut Moeljatno, ialah:[92]

1. Kemampuan bertanggungjawab
2. Kesalahan dalam arti luas (sengaja dan kelalaian)
3. Tidak adanya alasan pemaaf.

---

[89] Saleh, *Op. Cit*. Hlm.75
[90] Amrani & Ali, *Op. Cit*. Hlm.22
[91] *Ibid*.
[92] Moeljatno, *Perbuatan Pidana dan Pertanggungjawaban Pidana* (Yogyakarta: Universitas Gadjah Mada, 1989). Hlm.90

Menurut Van Hammel, terdapat 3 syarat yang harus di penuhi oleh seseorang agar dapat dikatakan mampu bertanggungjawab, yaitu:[93]

1) Bahwa orang tersebut mampu untuk menginsyafi arti perbuatannya dalam hal makna dan akibat sungguh-sungguh dari perbuatannya sendiri;
2) Bahwa orang mampu untuk menginsyafi perbuatannya itu bertentangan dengan ketertiban masyarakat;
3) Bahwa orang itu mampu menentukan kehendaknya terhadap perbuatannya itu.

2.5 Kebijakan Formulasi

Tahap formulasi adalah suatu tahap penegakan hukum secara *in abstracto* oleh badan legislatif atau pembuat undang-undang. Pada tahap ini sering disebut dengan tahap legislatif atau kebijakan legislatif. Menurut Barda Nawawi Arief dalam Dey Ravena dan Kristian menyatakan bahwa, kebijakan legislatif adalah suatu perencanaan atau program dari pembuat undang-undang mengenai apa yang akan dilakukan dalam menghadapi problem tertentu dan cara bagaimana melakukan atau melaksanakan sesuatu yang telah direncanakan atau diprogramkan itu.[94]

H.L. Packer memberikan pendapat bahwa kebijakan legislatif dalam bidang hukum *panitensier* sangat penting bagi suatu kebijakan pemidanaan *(sentencing policy)*. Kebijakan pemidanaan ini merupakan salah satu masalah kontroversial saat ini dalam hukum pidana.[95]

---

[93] Soedarto, *Pengetahuan Dasar Hukum Pidana* (Bandung: Mandar Maju, 2005). Hlm.18
[94] Ravena, *Op. Cit*. Hlm.147
[95] *Ibid*. Hlm.148

Pokok-pokok kebijakan formulasi dalam hukum pidana terdiri dari beberapa hal, yaitu:[96]

a. Permusan Tindak Pidana (*criminal Act*)

Tindak pidana adalah suatu perbuatan yang pelakunya dapat dijatuhi pidana. Perumusan tindak pidana harus terdapat unsur perbuatan seseorang. Pada dasarnya, yang dapat melakukan tindak pidana ialah orang atau manusia, tetapi seiring perkembangan jalan muncul subjek hukum baru yaitu korporasi yang dinilai dapat melakukan tindak pidana dan dapat dijatuhi pertanggungjawaban secara pidana. Unsur lain dalam tindak pidana ialah perbuatan. Perbuatan yang dapat dikenakan pidana ialah perbuatan yang melawan hukum yang memenuhi rumusan delik sebagaimana dirumuskan dalam undang-undang. Perbuatan tersebut dapat berupa berbuat atau tidak berbuat. Selain melawan hukum, perbuatan tersebut juga harus merugikan masyarakat, artinya bertentangan atau menghambat terlaksananya tata tertib dalam pergaulan bermasyarakat. Roeslan saleh menyatakan bahwa perbuatan pidana adalah perbuatan antisosial. Perbuatan seseorang dikatakan tindak pidana apabila perbuatan tersebut diatur dalam undang-undang. Dapat dikatakan bahwa untuk mengetahui apakah perbuatan tersebut tindak pidana atau bukan, maka harus dilihat dari rumusan-rumusan undang-undang. Hal tersebut berdasarkan pada asas *legalitas* yang terdapat dalam Pasal 1 ayat (1) KUHP yaitu tidak ada perbuatan yang dilarang dan

[96] *Ibid*. Hlm.148-156

diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam peraturan perungdang-undangan.

b. Perumusan Pertanggungjawaban Pidana (*Criminal Responsibility* atau *Criminal Liability*)

Seseorang yang telah melakukan tindak pidana belum tentu dapat dipidana karena sebelum menentukan terdakwa dipidana, harus terlebih dahulu memenuhi 2 syarat yaitu apakah perbuatan tersebut merupakan tindak pidana dan apakah pelaku tersebut dapat dipertanggungjawabkan atau tidak. Menentukan suatu tindak pidana harus berdasarkan pada asas *legalitas* sedangkan untuk menetukan adanya pertanggungjawaban pidana didasarkan pada asas kesalahan. Asas *legalitas* berkaitan dengan tindak pidana sedangkan asas kesalahan berkaitan dengan orang yang berbuat dan sikap batin jahat yang dimiliki oleh orang tersebut. Pertanggungjawaban pidana dimaksudkan untuk apakah seseorang dapat dipertanggungjawabkan atas suatu tindak pidana atau tidak. Inggris mengenal doktrin atau teori *strict liability* yang berarti bahwa untuk tindak pidana tertentu pada suatu tindak pidana tidak diperlukan adanya *mens rea. Mens rea* adalah *subjective guilt* yang melekat pada si pelaku. *Subjective guilt* meliputi kesengajaan atau kealpaan. Dalam sistem hukum pidana nasional, doktrin atau teori *strict liability* atau pertanggungjawaban ketat telah diatur secara tegas dalam Rancangan Kitab Undang-undang Hukum Pidana tahun 2015 yang terdapat dalam Pasal 38 ayat (1).

c. Perumusan Sanksi (*sanction*) baik yang berupa pidana maupun yang berupa tindakan tata tertib.

Salah satu usaha penanggulangan kejahatan dengan menggunakan hukum pidana yaitu dengan sanksi pidana. Sanksi pidana dapat dikatakan sanksi yang paling kejam dibandingkan sanksi perdata dan sanksi administrasi. Roeslan saleh menyatakan bahwa pidana adalah reaksi atas delik dan ini berujud suatu nestapa yang dengan sengaja ditimpakan negara pada pembuat delik. Van Bemmelen juga menyatakan bahwa hukum pidana menentukan sanksi terhadap pelanggaran peraturan larangan. Sanksi itu pada prinsipnya terdiri atas penambahan penderitaan yang dilakukan dengan sengaja. Berkaitan dengan tahap formulasi atau kebijakan formulasi, maka pemberian pidana menyangkut pembentuk undang-undang yang menetapkan *stelsel* sanksi hukum pidana dalam perundang-undangan yang dibuat. Dalam menetukan *stelses* sanksi ataupun sistem sanksi tidak hanya menetapkan susunan jenis-jenis pidana, berat ringannya sanksi, dan cara melaksanakan pidana tetapi harus memperhatikan juga aliran-aliran yang terdapat dalam hukum pidana dan tujuan pemidanaan. Muladi menyatakan, untuk menetapkan sistem sanksi tersebut akan sangat berkaitan dengan tiga permasalahan pokok hukum pidana yaitu tindak pidana, pertanggungjawaban pidana, dan perumusan sanksi pidana. Saat ini, perumusan sanksi pidana telah mengalami perkembangan, sanksi pidana tidak lagi bersifat menderita tetapi juga dapat berupa tindakan bahkan bersifat restoratif. Terkait dengan sanki pidana yang bersifat restoratif,

sanksi ini berasal dari konsep keadilan restoratif *(restorative justice)* yang memandang tindak pidana bukan sebagai pelanggaran terhadap hukum negara melainkan memandang tindak pidana sebagai pelanggaran seseorang terhadap orang lain dan diakui sebagai konflik. Reorientasi dan re-evaluasi terhada masalah pidana dan pemidanaan khususnya melalui peraturan perundang-undangan sebagai salah satu hasil dari proses legislatif, merupakan suatu hak yang diperlukan sehubungan dengan perkembangan masyarakat dan meningkatnya kriminalitas di Indonesia dan Internasional. Maka, penetapak sanksi pidana dalam perundang-undangan tidak dapat dilepaskan sebagai salah satu tujuan untuk menekan dan menanggulangi masalah kejahatan yang terjadi di masyarakat.

Kebijakan formulasi tidak dapat lepas dari kriminalisasi. Menurut pendapat yang dikemukakan oleh Barda Nawawi Arief, beliau menyatakan bahwa kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana).[97] Hal tersebut sejalan dengan Sudarto sebagaimana dikutip oleh Widodo, kriminalisasi adalah proses penetapan suatu perbuatan orang sebagai suatu tindak pidana, yang mana proses tersebut diakhiri dengan terbentuknya undang-undang yang mengatur bahwa perbuatan tersebut merupakan tindak pidana dan diancam dengan pidana.[98] Jadi, teori kebijakan kriminalisasi adalah proses penetapan suatu perbuatan yang awal nya bukan merupakan tindak pidana menjadi suatu perbuatan tindak pidana dan diancam

[97] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara, Op. Cit*. Hlm.57
[98] *Ibid*.

dengan pidana dan berakhir dengan dibentuknya suatu undang-undang yang mengatur perbuatan tersebut. Dalam hal ini, yang dimaksud dengan kriminalisasi *"cybercrime"* sebenarnya adalah kriminalisasi perbuatan-perbuatan yang dilakukan dalam dunia *cyber (cyberspace)*.[99]

Dalam hal melakukan kriminalisasi harus memperhatikan beberapa hal berikut:[100]

1. Penggunaan hukum pidana perlu memperhatikan tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil dan makmur yang merata baik material maupun spiritual berdasarkan Pancasila. Penggunaan hukum pidana ditujukan untuk menanggulangi kejahatan dan mengadakan peng-*ugeran* terhadap tindakan penanggulangan itu sendiri, demi kesejahteraan dan pengayoman masyarakat.
2. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana seyogyanya merupakan perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian (material dan/atau spiritual) pada warga masyarakat.
3. Penggunaan hukum pidana perlu memperhitungkan prinsip "biaya dan hasi" *(cost and benefit principle)*.
4. Penggunaan hukum pidana perlu pula memperhitungkan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum pidana, jangan sampai ada kelebihan beban tugas *(overbelasting)*.

[99] *Ibid*.
[100] *Ibid*. Hlm.58

2.6 Konsep tentang Kejahatan

Hoefnagels dalam M. Arief Amrullah menyatakan kejahatan adalah suatu pengertian yang relatif, maksudnya ialah banyak pengertian yang digunakan dalam ilmu-ilmu sosial yang berasal dari bahasa sehari-sehari tetapi terjadi perbedaan dalam pengartiannya.[101] Perilaku menyimpang dari seseorang tertentu dipandang sebagai kejahatan, yaitu apabila perbuatan tersebut dirasakan sebagai perbuatan yang serius dan tercela, tetapi perbuatan yang sama mungkin tidak dianggap sebagai kejahatan apabila terjadinya dalam konteks yang berbeda.[102]

Namun demikian, sebagaimana yang ditulis oleh Hoefnagels seperti yang dikutip oleh M. Arief Amrullah, apabila memperhatikan unsur-unsur dari kejahatan *(crime)* yang dalam bahasa Belanda disebut *misdaad*, dalam bahasa Jerman disebut *missetaat*, dan dalam bahasa Inggris disebut *misdeed*, dalam bahasa sehari-hari dari beberapa negara, sebagai contoh perbuatan yang sangat tercela biasanya perbuatan yang dapat dipidana, hal tersebut sering di pandang sebagai kejahatan dalam beberapa hukum pidan.[103]

Howard Abadinsky juga memberikan penjelasan mengenai kejahatan, menurut kejahatan sering sering dipandang sebagai *mala in se* atau *mala prohibita* (*mala in se* menunjuk kepada perbuatannya yang pada hakikatnya adalah kejahatan contohnya pembunuhan, sedangkan *mala prohibita* merujuk pada

---

[101] M Arief Amrullah, *Politik Hukum Pidana (perlindungan korban kejahatan ekonomi di bidang perbankan dalam perspektif bank sebagai pelaku (offender))*, revisi ed (Yogyakarta: Genta Publishing, 2015). Hlm.25

[102] *Ibid*.

[103] *Ibid*.

perbuatan yang hanya ditetapkan oleh oleh negara sebagai perbuatan yang dilarang).[104]

Sahetapy dan Mardjono Reksodiputro sebagaimana dikutip oleh M. Arief Amrullan, menyatakan bahwa kejahatan mengandung konotasi tertentu, merupakan suatu pengertian dan penamaan yang relatif, mengandung variabelitas dan dinamik serta bertalian dengan perbuatan atau tingkah laku, baik aktif maupun pasif yang dinilai oleh sebagai mayoritas atau minoritas masyarakat sebagai suatu perbuatan anti sosial, suatu perkosaan terhadap skala nilai sosial dan atau dengan perasaan hukum yang hidup dalam masyarakat sesual dengan ruang dan waktu.[105]

Mardjono Reksodiputro juga menyatakan bahwa, sebagian masyarakat Indonesia mengartikan kejahatan sebagai pelanggaran atas hukum pidana, baik dalam undang-undang maupun dalam perundang-undangan administrasi yang bersanksi pidana.[106] Persepsi yang demikian ini, berarti kejahatan mendahului hukum, artinya suatu perbuatan yang dianggap sangat merugikan masyarakat, kemudian muncul hukum pidana yang bertujuan melindungi kepentingan masyarakat.[107] Selain itu, Reksodiputro juga menyatakan bahwa ada pula yang mengartikan suatu perbuatan tertentu sebagai suatu kejahatan karena hukum yang menyatakan demikian.[108]

---

[104] *Ibid*.
[105] *Ibid*. Hlm.26
[106] *Ibid*. Hlm.27
[107] *Ibid*.
[108] *Ibid*.

2.7 Teori Anomie

Teori adalah seperangkat konsep yang saling terkait, definisi, dan proposisi yag menyajikan pandangan sistematis atas fenomena yang menentukan hubungan antar-variael, dengan tujuan menjelaskan dan memprediksi fenomena tersebut.[109] Kriminologi adalah studi tentang mengapa seseorang (individu) melakukan kejahatan dan mengapa mereka berperilaku dalam situasi tertentu, melalui pemahaman tersebut seseorang dapat mengembangkan cara untuk mengendalikan kejahatan atau merehabilitasi penjahat.[110]

Kriminologi juga merupakan ilmu yang mempelajari tentang kebijakan pemberantasan kejahatan, konsepsi kejahatan, penyebab terjadinya kejahatan, bentuk-bentuk kejahatan, *modus* kejahatan, dan upaya penanggulangan kejahatan.[111] Teori kriminologi akan membantu manusia memahami mekanisme kerja sistem peradilan pidana dan pemegang peran dalam sistem peradilan pidana, sebuah teori dapat mencoba menjelaskan kejahatan pada lingkup masyarakat luas (makro), atau juga menjelaskan kejahatan pada lingkup inividu (mikro).[112]

Teori kriminologi yang digunakan sebagai pisau analisis dalam tesis ini ialah teori anomi *(anomy theory)*. Teori anomi ini dikemukan oleh sosiolog Perancis yang bernama Emille Durkhein (1858-1917) dan Robert Merton. Durkheim menggunakan istilah anomi untuk menyebut suatu kondisi yang mengalami deregulasi. Menurut Durkheim perubahan sosial yang cepat dalam

---

[109] Widodo, *Memerangi Cybercrime (Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi)*, 1st ed (Yogyakarta: Aswaja Pressindo, 2013). Hlm.52

[110] *Ibid*.

[111] *Ibid*. Hlm.53

[112] *Ibid*.

masayarakat mempunyai pengaruh yang besar dalam kelompok masyarakat yang menyebabkan nilai-nilai yang ada dalam masyarakat menjadi kabur bahkan lenyap sehingga mendorong ketidak pastian norna atau bahkan ketiadaan norma.[113] Durkheim menggambarkan konsep anomi sebagai kondisi dalam masyarakat yang terjadi keputusasaan atau ketiadaaan norma. Selain itu anomi juga merupakan akibat perubahan bermasyarakat yang cepat.

Robert Merton mengungkapkan bahwa perilaku menyimpang dianggap sebagai suatu tingkah laku abnormal karena perilaku tersebut berpangkal pada individu.[114] Robert Merton juga menganggap bahwa tingkah laku yang melanggar norma disebabkan oleh gangguan dan tekanan sosial yang memunculkan ketidakselarasan antara tujuan dengan cara untuk mencapai tujuan tersebut.[115] Kondisi seperti inilah yang memicu munculnya perilaku menyimpang, dan kondisi inilah yang disebut dengan kondisi anomi.

Romli Atmasasmita memberikan penjelasan mengenai perbedaan teori anomi Durkheim dan teori anomi Merton. Teori anomi Durkheim menitikberatkan pada ketiadaan norma tanpa menjelaskan sebab-sebab terjadinya ketiadaan norma, sedangkan teori anomi Merton menitikberatkan pada *differencial acces to opportunity structure*.[116] Jadi, dapat disimpulkan bahwa teori anomi adalah teori yang beranggapan bahwa kejahatan tersebut muncul karena dalam masyarakat tidak ada norma yang mengatur suatu aktivitas tersebut *(normlesness)*.[117]

---

[113] *Ibid*. Hlm.66
[114] *Ibid*. Hlm.67
[115] *Ibid*.
[116] *Ibid*. Hlm.69
[117] *Ibid*. Hlm.83

2.8 Asas Legalitas

Perkara pidana harus memperhatikan asas-asas hukum pidana yang berlaku agar tidak mengurangi hak asasi dari orang lain. *"nullum delictum nulla poena sine previa legi poenali"* atau asas legalitas merupakan salah satu asas yang penting dalam hukum pidana. Asas tersebut mengatur mengenai "suatu perbuatan tidak dapat dipidana, kecuali berdasarkan ketentuan-ketentuan perundang-undangan pidana yang telah ada". Asas legalitas terdapat dalam aturan hukum yaitu Pasal 1 Ayat (1) Kitab Undang-undang Hukum Pidana yang menentukan "tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada, sebelum perbuatan tersebut dilakukan. Pada umumnya, para ahli hukum pidana sepakat dengan adanya 3 (tiga) makna dalam asas legalitas, yaitu:[118]

1) Tidak ada perbuatan yang dilarang dan diancam dengan pidana kalau hal itu belum dinyatakan terlebih dahulu dalam suatu aturan undang-undang;
2) Untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi; dan
3) Aturan-aturan hukum pidana tidak berlaku surut.

Pemahaman makna asas legalitas sejatinya telah mengalami beberapa perkembangan, hal tersebut tampak dalam beberapa tahap yaitu sebagai jaminan dari tindakan.

---

[118] Deni Setyo Bagus Yuherawan, *Dekonstruksi Asas Legalitas Hukum Pidana (sejarah asas legalitas dan gagasan pembaharuan filosofis hukum pidana)*, 1st ed (Malang: Setara Press, 2014). Hlm.5

BAB 3

KERANGKA KONSEPTUAL

Dalam hal ini penyusunan tesis sebagai penelitian hukum adalah terhadap masalah bagaimana hukum pidana dapat mengkriminalisasi kejahatan *cybersquatting*, terutama dalam hal pertanggungjawaban pelakunya. Karena dalam Undang-undang Nomor 19 Tahun 20016 tentang Informasi dan Transaksi Elektronik tidak mengatur secara khusus dan jelas mengenai kejahatan *cybersquatting*.

Kejahatan *cybersquatting* sendiri terjadi di beberapa negara, salah satunya Indonesia. Kejahatan *cybersquatting* berhubungan erat dengan *domain name*. Tidak diaturnya kejahatan *cybersquatting* dalam hukum nasional memungkinkan pelaku sulit dipertanggungjawabkan secara pidana dalam Undang-Undang Informasi dan Transaksi Elektronik. Adanya KUHP dan Undang-Undang Informasi dan Transaksi Elektronik ternyata tidak membuat pelaku kejahatan *cybersquatting* jera. Untuk menanggulangi kejahatan *cybersquatting* tersebut, maka dibutuhkan upaya secara penal dan non-penal. Penanggulanangan secara penal dapat dilakukan dengan memasukkan kejahatan *cybersquatting* dalam Undang-Undang Informasi dan Transaksi Elektronik sehingga para pelaku kejahatan *cybersquatting* dapat dipertanggungjawabkan secara pidana.

Berkaitan dengan pertanggungjawaban pidana, sistem pertanggungjawaban pidana dalam hukum nasional Indonesia menganut asas kesalahan sebagai salah satu asas di samping asas legalitas. Pertanggungjawaban

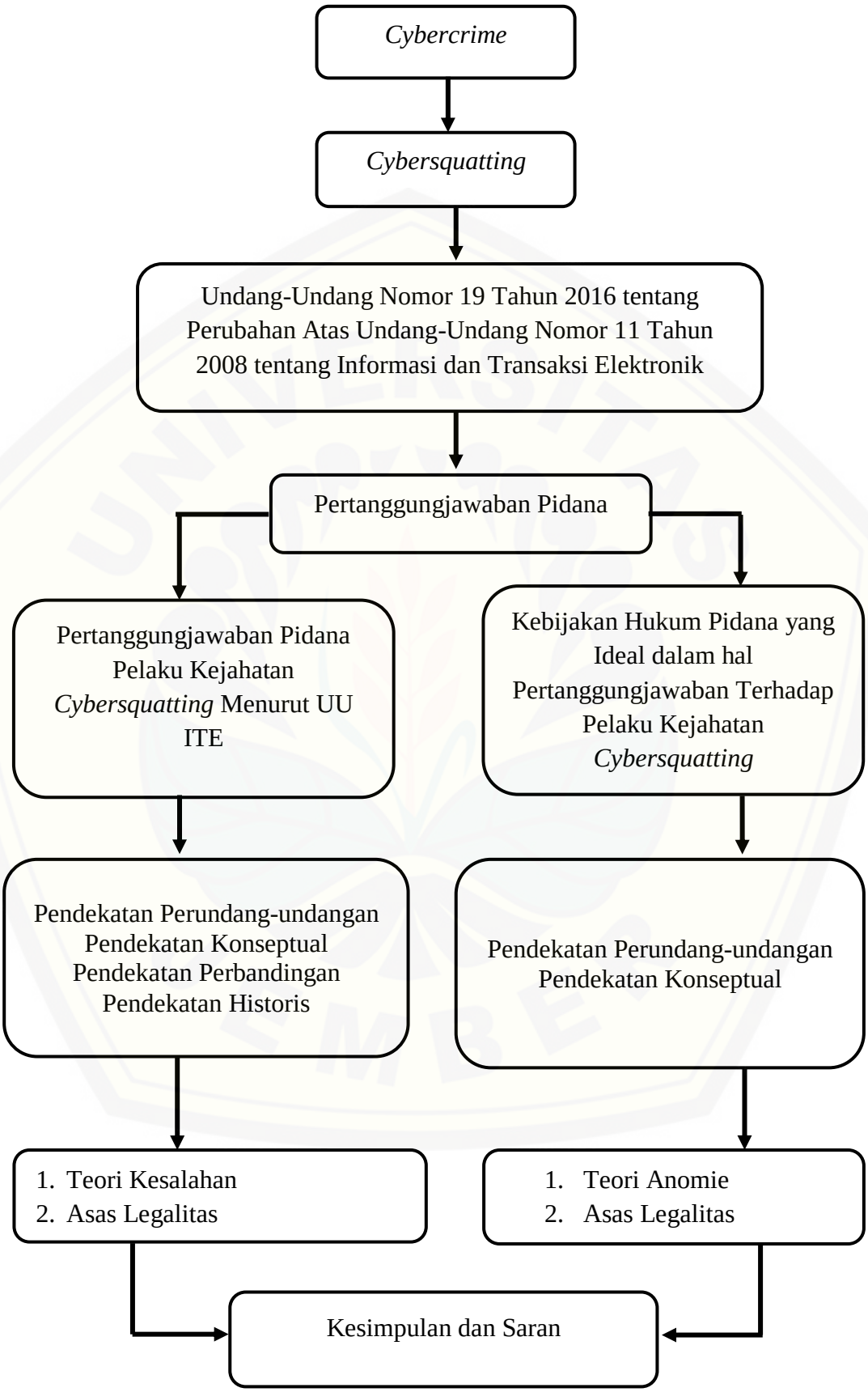
dan fungsi preventif sejatinya dapat dihubungkan satu sama lain. Konsep tersebut harus dapat menyadari pelaku/pembuat bahwa dalam perbuatannya terdapat konsekuensi hukum yang harus diterima. Artinya, konsekuensi hukum tersebut merupakan risiko yang harus diterima oleh pelaku kejahatan. Pertanggungjawaban pidana adalah pertanggungjawaban yang diajtuhkan kepada pelaku atas perbuatan tindak pidana yang dilakukan. Artinya, yang dipertanggungjawabkan itu ialah tindak pidana yang dilakukannya.[119] Adanya tindak pidana atau perbuatan pidana yang dilakukan merupakan awal timbulnya pertanggungjawaban pidana. Dapat dikatakan bahwa tidak mungkin ada pertanggungjawaban pidana jika tidak melakukan tindak pidana. Faktor kesalahan merupakan faktor yang sangat penting dalam hal penjatuhan pidana terhadap pelaku. Jadi, pertanggungjawaban pidana berkaitan erat dengan faktor kesalahan yang ada pada diri pelaku.

Pertanggungjawaban pidana terhadap pelaku kejahatan *cybersquatting* adalah salah satu hal penting yang harus diatur lebih lanjut dan merupakan upaya penal dalam hal penanggulangan kejahatan *cybersquatting*. Sehingga pelaku kejahatan *cybersquatting* dapat dipertanggungjawabkan secara pidana.

Beberapa teori, asas, dan konsep yang gunakan sebagai pisau analisis dalam membahas rumusan masalah dalam kaitannya dengan *cybersquatting* ialah konsep kebijakan hukum pidana, konsep kriminalisasi, teori kesalahan, teori anomie, dan asas legalitas. Teori kesalahan dan asas legalitas digunakan sebagai pisau analisis pada rumusan masalah yang pertama. Sedangkan konsep kebijakan hukum pidana, teori anomie, dan konsep kriminalisasi digunakan sebagai pisau

[119] Choirul Huda, *Dari TIada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan* (Jakarta: Kencana, 2006). Hlm.62

analisi pada rumusan masalah yang kedua. Pembahasan dan hasil analisis dari masing-masing rumusan masalah akan menghasilkan kesimpulan dan saran sebagaimana diuraikan dalam bagan berikut ini:



BAB 5

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan dalam bab terdahulu, didapatlan kesimpulan sebagai berikut:

1. Teori kesalahan yang terdapat dalam pertanggungjawaban pidana memberikan beban pada korban untuk membuktikan bahwa pelaku melakukan perbuatan yang melawan hukum. Teori tersebut pada dasarnya telah dianut oleh Undang-Undang ITE. Terkait pertanggungjawaban pelaku dalam kejahatan *cybersquatting* berlaku adanya kesalahan. Akan tetapi, pertanggungjawaban pidana dalam Undang-Undang ITE saat ini tidak dapat diterapkan terhadap kejahatan *cybersquatting*. Hal tersebut dikarenakan belum diatur nya kejahatan *cybersquatting* dalam Undang-Undang ITE dan berakibat pelaku kejahatan *cybersquatting* tidak dapat dipertanggungjawabkan atas perbuatannya. Apabila Undang-Undang ITE diterapkan terhadap pelaku kejahatan *cybersquatting* jelas akan bertentang dengan asas legalitas. Indonesia dapat juga mencontoh Amerika Serikat dalam hal pertanggungjawaban terhadap pelaku kejahatan *cybersquatting*. Jika Amerika hanya memberikan pertanggungjawaban berupa denda, maka Indonesia dapat menambahkan pidana penjara terhadap pelaku untuk memberikan efek jera dan rasa takut bagi para pelaku selanjutnya.
2. Teori anomie yang dikemukan oleh durkheim menyatakan bahwa suatu kejahatan itu muncul karena tidak ada norma yang mengaturnya. Oleh

karena itu sangat diperlukan suatu kebijakan formulasi terhadap kejahatan *cybersquatting.* Kebijakan formulasi pertanggungjawaban pidana yang ideal terhadap pelaku kejahatan *cybersquatting* di masa yang akan datang telah tercantum dalam RKUHP Tahun 2015 dan RKUHP Tahun 2017 melalui proses kriminalisasi terhadap kejahatan *cybersquatting* dengan menentukan aturan mengenai sistem pidana dan pemidanaannya, sehingga pertanggungjawaban pidana dapat dibebankan kepada pelaku kejahatn *cybersquatting*. Seiring dengan proses kriminalisasi terhadap kejahatan *cybersquatting*, maka tidak terdapat pelanggaran asas legalitas dalam penerapannya kelak.

5.2 Saran

Bertitik tolak pada permasalahan yang ada dan dikaitkan dengan kesimpulan di atas, dapat diberikan saran sebagai berikut:

1. Hukum positif Indonesia saat ini masih mempunyai keterbatasan dalam hal pertanggungjawaban pidana terhadap pelaku kejahatan *cybersquatting* dikarenakan Undang-Undang ITE yang ada saat ini tidak memadai untuk diaplikasikan terhadap kejahatan *cybersquatting*, jadi diperlukan suatu pembaharuan terhadap Undang-Undang ITE kita.
2. Perlu segera dibahas dan disahkan mengenai RKUHP supaya pertanggungjawaban pidana dapat dibebankan kepada pelaku kejahatan *cybersquatting* dan untuk meningkatkan kemampuan hukum pidana dalam pemberantasan kejahatan *cybersquatting* di Indonesia.

DAFTAR PUSTAKA

A. BUKU

Amrani, Hanafi & Mahrus Ali. *Sistem Pertanggungjawaban Pidana Perkembangan dan Penerapan*, 1st ed (Jakarta: PT. RajaGrafindo Persada, 2015).

Amrullah, M Arief. *Politik Hukum Pidana (perlindungan korban kejahatan ekonomi di bidang perbankan dalam perspektif bank sebagai pelaku (offender))*, revisi ed (Yogyakarta: Genta Publishing, 2015).

Anwar, Yesmil & Adang. *Kriminologi*, 1st ed (Bandung: PT. Refika Aditama, 2010).

Arief, Barda Nawawi. *Kebijakan Hukum Pidana, Perkembangan Penyusunan Konsep KUHP Baru* (Jakarta: Kencana, Prenada Media Group, 2008).

———. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, 4th ed (Jakarta: Kencana, Prenada Media Group, 2014).

Atmasasmita, Romli. *Asas-asas Perbandingan Hukum Pidana*, 1st ed (Jakarta: Yayasan LBH, 1989).

Dirdjosisworo, Soedjono. *Hukum Perusahaan Mengenai Hak Atas Kekayaan Intelektual (Hak Cipta, Hak Paten, Hak Merek)* (Bandung: Mandar Maju, 2000).

Eddyono, Supriyadi Widodo et al. *Melihat rencana kodifikasi dalam RKUHP: tantangan upaya pembaruan hukum di Indonesia* (2015).

Garner, Bryan A. *Black's Law Dictionary*, 10th ed (United States of Amerika: Thomson Reuters, 2014).

Huda, Choirul. *Dari TIada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan* (Jakarta: Kencana, 2006).

Ibrahim, Johnny. *Teori dan Metodelogi Penelitian Hukum Normatif*, 2d ed (Malang: Banyumedia Publishing, 2006).

Kelsen, Hans. *Teori Umum Tentang Hukum dan Negara* (Bandung: Nusa Media, 2016).

Marzuki, Peter Mahmud. *Penelitian Hukum* (Jakarta: Kencana Media Group, 2013).

———. *Penelitian Hukum*, 9th ed (Jakarta: Prenadamedia Group, 2014).

Maskun. *Kejahatan Siber (Cyber Crime)*, 1st ed (Jakarta: Kencana, Prenada Media Group, 2013).

Moeljatno. *Perbuatan Pidana dan Pertanggungjawaban Pidana* (Yogyakarta: Universitas Gadjah Mada, 1989).

———. *Asas-Asas Hukum Pidana*, revisi ed (Jakarta: PT. Rineka Cipta, 2008).

Muladi & Barda Nawawi Arief. *Teori-teori dan Kebijakan Hukum Pidana*, 4th ed (Bandung: PT. Alumni, 2010).

Raharjo, Agus. *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: Citra Aditya Bhakti, 2002).

Ravena, Dey & Kristian. *Kebijakan Kriminal (Criminal Policy)*, 1st ed (Jakarta: Kencana, Prenada Media Group, 2017).

Saleh, Roeslan. *Perbuatan Pidana dan Pertanggungjawaban Pidana; Dua Pengerrtian Dasar dalam Hukum Pidana*, 3d ed (Jakarta: Aksara Baru, 1983).

Sjawie, Hasbullah F. *Pertanggungjawaban Pidana Korporasi Pada Tindak Pidana Korupsi*, 1st ed (Jakarta: Prenadamedia Group, 2015).

Soedarto. *Pengetahuan Dasar Hukum Pidana* (Bandung: Mandar Maju, 2005).

Soemitro, Ronny Hanitijo. *Metode Penelitian Hukum dan Jurimetri* (Jakarta: Rinneka Cipta, 1988).

Tampubolon, Sabartua. *Aspek Hukum Nama Domain di Internet*, 1st ed (Jakarta: PT. Tatanusa, 2003).

Wahid, Abdul & Mohammad Labib. *Kejahatan Mayantara (cybercrime)* (Jakarta: PT. Refika Aditama, 2005).

widodo. *Sistem Pemidanaan dalam Cyber Crime (alternatif ancaman pidana, kerja sosial dan pidana pengawasan bagi pelaku cyber crime)*, 1st ed (Yogyakarta: Laksbang Mediatama, 2009).

Widodo. *Hukum Pidana di Bidang Teknologi Informasi. Cybercrime Law: Telaah Teoritik dan Bedah Kasus*, 1st ed (Yogyakarta: Aswaja Pressindo, 2013).

———. *Aspek Hukum Pidana Kejahatan Mayantara*, 1st ed (Yogyakarta: Aswaja Pressindo, 2013).

———. *Memerangi Cybercrime (Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi)*, 1st ed (Yogyakarta: Aswaja Pressindo, 2013).

Wisnubroto, Al. *Strategi Penanggulangan Kejahatan Telematika*, 1st ed (Yogyakarta: Atma Jaya Yogyakarta, 2010).

Yuherawan, Deni Setyo Bagus. *Dekonstruksi Asas Legalitas Hukum Pidana (sejarah asas legalitas dan gagasan pembaharuan filosofis hukum pidana)*, 1st ed (Malang: Setara Press, 2014).

Zaidan, M Ali. *Kebijakan Kriminal*, 1st ed (Jakarta: Sinar Grafika, 2016).

B. JURNAL

Basile, Jr, Andrew R. "Risghts to Domain Names" (1996) Online Law SPAs Leg Guide Doing Bus Internet 227.

Jain, Sankalp. "Cybersquatting: Concept, Types and Legal Regimes in India & USA" (2015) 20.

Moore, M. "Cybersquatting: Prevention better than cure?" (2009) 17:2 Int J Law Inf Technol 220.

C. MAJALAH, TESIS, dan INTERNET

Hairi, Prianter Jaya. "Model Kodifikasi Dalam RUU KUHP", *Maj Info Singk Huk Kaji Singk Terhadap Isu Aktual Dan Strateg* (September 2016).

Nizar, Muhammad. *Kejahatan Nama Domain yang Berkaitan dengan Merek Ditinjau Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* Universitas Airlangga, 20017)

Priyanto, Yoga Tri. "Kontroversi cybersquatting menyerang Indonesia dan Traveloka", (12 November 2003), online: *Kontroversi Cybersquatting Menyerang Indones Dan Travel* <https://www.merdeka.com/teknologi/kontroversi-cybersquatting-menyerang-indonesia-dan-traveloka.html>.

"Tentang Pandi", online: <https://pandi.id/profil/tentang-pandi/>.

"Cybersquatting", online: *Law Teach Law Essay Prof* <https://www.lawteacher.net/free-law-essays/business-law/business-law-law-essays.php#>.