TESIS

KEBIJAKAN INTEGRAL HUKUM PIDANA DENGAN *TECHNO PREVENTION* DALAM UPAYA PENCEGAHAN KEJAHATAN *CYBERBULLYING*

INTEGRAL POLICY CRIMINAL LAW WITH TECHNO PREVENTION IN PREVENTING CYBERBULLYING CRIME

FIRDA LAILY MUFID, S.H.
NIM : 150720101011

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS JEMBER
PROGRAM STUDI MAGISTER HUKUM
2017

TESIS

KEBIJAKAN INTEGRAL HUKUM PIDANA DENGAN *TECHNO PREVENTION* DALAM UPAYA PENCEGAHAN KEJAHATAN *CYBERBULLYING*

INTEGRAL POLICY CRIMINAL LAW WITH TECHNO PREVENTION IN PREVENTING CYBERBULLYING CRIME

FIRDA LAILY MUFID, S.H.
NIM : 150720101011

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS JEMBER
PROGRAM STUDI MAGISTER HUKUM
2017

KEBIJAKAN INTEGRAL HUKUM PIDANA DENGAN *TECHNO PREVENTION* DALAM UPAYA PENCEGAHAN KEJAHATAN *CYBERBULLYING*

INTEGRAL POLICY CRIMINAL LAW WITH TECHNO PREVENTION IN PREVENTING CYBERBULLYING CRIME

TESIS

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

Oleh :

FIRDA LAILY MUFID, S.H.
NIM : 150720101011

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS JEMBER
PROGRAM STUDI MAGISTER HUKUM
2017

PERSETUJUAN

TESIS INI TELAH DISETUJUI

TANGGAL.....

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 INTEGRAL HUKUM PIDANA DENGAN *TECHNO PREVENTION* DALAM UPAYA PENCEGAHAN KEJAHATAN *CYBERBULLYING*

Oleh :

FIRDA LAILY MUFID, S.H.
NIM : 150720101011

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

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

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

PENETAPAN PANITIA PENGUJI

Judul Tesis	: Kebijakan Integral Hukum Pidana dengan *Techno Prevention* dalam Upaya Pencegahan Kejahatan *Cyberbullying*
Tanggal Ujian	: 20 Juli 2017
S.K. Penguji	: .....
Nama Mahasiswa	: Firda Laily Mufid, S.H.
NIM	: 150720101011
Program Studi	: Magister Hukum

Komisi Pembimbing	:
Pembimbing Utama	: Prof. Dr. M. Arief Amrullah, S.H, M.Hum.
Pembimbing Anggota	: Dr. Fanny Tanuwijaya, S.H., M.Hum.

Tim Dosen Penguji	:
Dosen Penguji 1	: Dr. Jayus, S.H, M.Hum.
Dosen Penguji 2	: Dr. Y.A. Triana Ohoiwutun, S.H., M.H.
Dosen Penguji 3	: Prof. Dr. M. Arief Amrullah, S.H, M.Hum.
Dosen Penguji 4	: Dr. Fanny Tanuwijaya, S.H., M.Hum.
Dosen Penguji 5	: Dr. Dyah Ochtorina S. S.H, M.Hum

PENETAPAN PANITIA PENGUJI

Dipertahankan dihadapan Panitia Penguji pada :

Hari : Kamis
Tanggal : 20
Bulan : Juli
Tahun : 2107

Diterima oleh Panitia Penguji Fakultas Hukum Universitas Jember :

Ketua, **Sekretaris,**

Dr. Y.A. TRIANA OHOIWUTUN S.H., M.H.
NIP : 196310131990032001

Dr. JAYUS, S.H, M.Hum.
NIP : 195612061983031003

ANGGOTA PANITIA PENGUJI :

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

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

Dr. DYAH OCHTORINA S, S.H, M.Hum. **: (.....)**
NIP. : 198010262008122001

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 saksi lainnya yang berlaku di lingkungan Universitas Jember.

Jember, Juni 2017

Yang membuat pernyataan,

FIRDA LAILY MUFID, S.H.
NIM : 150720101011

UCAPAN TERIMA KASIH

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 Integral Hukum Pidana dengan *Techno Prevention* dalam Upaya Pencegahan Kejahatan *Cyberbullying***;** 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 2017. Pada kesempatan ini mengucapkan terima kasih 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. Jayus, S.H, M.Hum, selaku Ketua Panitia Penguji Tesis ;
4. Dr. Y.A. Triana Ohoiwutun, S.H., M.H., selaku Sekretaris Panitia Penguji Tesis ;
5. Dr. Nurul Ghufron, S.H., M.H, selaku Dekan, Dr. Dyah Ochtorina Susanti, S.H. M.Hum., selaku Penjabat Wakil Dekan I, Mardi Handono, S.H., M.H. dan Iwan Rachmad Soetijono, S.H., M.H, selaku Wakil Dekan II dan III Fakultas Hukum Universitas Jember ;
6. Bapak dan Ibu dosen, civitas akademika, serta seluruh karyawan Fakultas Hukum Universitas Jember atas segala ilmu dan pengetahuan yang diberikan ;
7. Orang tuaku, semua keluarga dan kerabat atas doa dan dukungan yang telah diberikan dengan setulus hati ;
8. Teman-teman seperjuangan di Program Magister Hukum Fakultas Hukum Universitas Jember angkatan tahun 2015 yang tak bisa aku sebutkan satu persatu yang telah memberikan dukungan dan bantuan baik moril dan spirituil ;
9. 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 skripsi ini minimal dapat menambah khasanah referensi serta bermanfaat bagi pembaca sekalian.

Jember, Juni 2017
Penulis,

FIRDA LAILY MUFID, S.H.
NIM : 150720101011

MOTTO

"Dan janganlah kamu mengikuti sesuatu yang tidak kamu ketahui. Sesungguhnya pendengaran, penglihatan dan hati, semuanya itu akan dimintai pertanggungjawaban" [QS Al-Israa : 36]

RINGKASAN

Teknologi informasi dan media elektronika dinilai sebagai simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial budaya, ekonomi dan keuangan. Dari sistem-sistem kecil lokal dan nasional, proses globalisasi dalam tahun-tahun terakhir bergerak cepat, bahkan terlalu cepat menuju suatu sistem global.

Perkembangan yang pesat dalam teknologi internet menyebabkan kejahatan-kejahatan di bidang teknologi informasi atau dapat disebut *cybercrime* atau *computer-related crime* yang semakin marak di Indonesia. *Cybercrime* adalah aktivitas manusia di dunia mayantara (maya) yang menjadikan komputer sebagai sasaran kejahatan (misalnya akses ilegal, perusakan situs, intersepsi ilegal), dan aktivitas manusia yang menggunakan komputer sebagai sasaran kejahatan (misalnya pemalsuan kartu kredit, pornografi *via* internet).

Salah satu kejahatan di dunia mayantara yakni *Cyberbullying* yang merupakan bentuk intimidasi yang dilakukan seseorang atau lebih untuk memojokkan, menyudutkan, orang lain melalui dunia *cyber*. Pengertian *cyberbullying* adalah penggunaan teknologi *internet* untuk menyakiti orang lain dengan cara sengaja dan diulang-ulang". Intimidasi ini tidak sembarangan akibatnya, tak jarang kematian menjadi akhir dari *cyberbullying*. *Cyberbullying* juga diartikan sebagai bentuk intimidasi yang pelaku lakukan untuk melecehkan korbannya melalui perangkat teknologi. Pelaku ingin melihat seseorang terluka, ada banyak cara yang mereka lakukan untuk menyerang korban dengan pesan kejam dan gambar yang mengganggu dan disebarkan untuk mempermalukan korban bagi orang lain yang melihatnya.

Berdasarkan uraian diatas permasalahan yang dibahas ada 2 (dua) yaitu : *Pertama*, Apakah dalam mencegah kejahatan *cyberbullying* akan dapat dicapai dengan menggunakan hukum pidana? *Kedua*, Bagaimana formulasi kebijakan integral hukum pidana dengan menggunakan sarana *Techno Prevention* sebagai upaya pencegahan kejahatan *cyberbullying* di masa yang akan datang?Metode penulisan yang digunakan penulis adalah yuridis normatif. Pendekatan masalah yang digunakan adalah pendekatan Undang – Undang (*statue approach*), pendekatan konseptual (*conceptual approach*) dan Pendekatan Historis (*Hystorical Approach*). Bahan sumber hukum yang digunakan adalah bahan hukum primer dan bahan hukum sekunder. Tujuan penelitian adalah Mengetahui dan memahami kebijakan integral hukum pidana dengan ilmu teknologi dapat digunakan sebagai upaya penanggulangan kejahatan *cyberbullying*; Mengetahui dan memahami penanggulangan kejahatan *cyberbullying* di masa yang akan datang.

Hasil kajian yang diperoleh bahwa: *Pertama* Pencegahan kejahatan *cyberbullying* secara menyeluruh belum dapat dicapai dengan sarana hukum pidana saat ini. Meskipun telah ada UU ITE, namun dalam pelaksanaannya banyak kendala yang dihadapi oleh penegak hukum. Hal ini karena terdapat beberapa keterbatasan

hukum pidana untuk mencegah kejahatan *cyberbullying*. Berkenaan dengan beberapa keterbatasan tersebut, kebijakan penerapan hukum pidana perlu diimbangi dengan kebijakan nonpenal. Bahkan kebijakan non penal mempunyai peranan yang sangat strategis dalam penanggulangan kejahatan *cyberbullying. Kedua,* Formulasi pencegahan *cyberbullying* didasarkan pada upaya menghilangkan sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan tersebut. Dalam mengsinergikan kebijakan penal dan non penal perlu adanya pendekatan yang berorientasi pada kebijakan (*policy oriented approach*). Permasalahan utama dalam mengintregasikan dan mengharmonisasikan kebijakan penal dengan nonpenal kearah penekanan dan pengurangan faktor-faktor potensial yang menumbuhsuburkan kejahatan. Melalui pendekatan intergral tersebut diharapkan pelaksanaan rencana perlindungan masyarakat (*social defence planning*) berhasil. Keberhasilan tersebut dapat menopang pencapaian tujuan kebijakan sosial yang tertuang dalam rencana pembangunan nasional.

Berdasarkan hasil kajian tersebut penulis memberikan saran, antara lain: *Pertama,* Hukum pidana masih mempunyai keterbatasan untuk menanggulangi kejahatan *cyberbullying*, maka dari itu penanggulangan tidak hanya dilakukan dengan mengaplikasikan Undang-undang saja. Seharusnya, upaya pencegahan non penal dengan menitikberatkan pada edukasi kepada masyarakat tentang kode etik menggunakan jejaring sosial. Selain itu, seharusnya pencegahan di bidang teknologi juga dengan meningkatkan kemanan sistem informasi. *Kedua,* Seharusnya perlu segera dibahas dan dibuat peraturan mengenai Tindak Pidana di bidang Teknologi Infomasi karena RUU ini dapat menjadi pelengkap UU ITE untuk lebih meningkatkan kemampuan hukum pidana dalam pemberantasan kejahatan *cyberbullying* di Indonesia.

SUMMARY

Information technology and electronic media are considered as pioneer symbols, which will integrate the entire world system, both in the socio-cultural, economic and financial aspects. From small local and national systems, the process of globalization in recent years is moving quickly, even too rapidly toward a global system.

The rapid development in internet technology led to crimes in the field of information technology or can be called cybercrime or computer-related crime is increasingly prevalent in Indonesia. Cybercrime is a human activity in the world mayantara (maya) that makes the computer as a target of crime (eg illegal access, destruction of sites, illegal interception), and human activities that use computers as crime targets (eg credit card fraud, pornography via the internet).

One crime in the world mayantara Cyberbullying which is a form of intimidation by someone or more to cornering, cornering, others through the cyber world. Understanding cyberbullying is the use of internet technology to harm others by way of deliberate and repetitive ". Intimidation is not arbitrary consequences, not infrequently the death to be the end of cyberbullying. Cyberbullying is also interpreted as a form of intimidation that perpetrators do to harass their victims through technological devices. The perpetrator wants to see someone hurt, there are many ways they do to attack the victim with cruel messages and disturbing and scattered images to embarrass the victim for others who see it.

Based on the above description of the issues discussed there are 2 (two), namely: First, Is in preventing cyberbullying crime will be achieved by using criminal law? Second, how is the formulation of integral policy of criminal law as effort of prevention of cyberbullying crime in the future? Writing method used by writer is normative juridical. The problem approach used is the statue approach, the conceptual approach and the Historical Approach. The legal source materials used are primary legal materials and secondary legal materials. The purpose of the study is to know and understand the integral policy of criminal law with the science of technology can be used as an effort to combat cyberbullying crime; Know and understand the prevention of cyberbullying crime in the future.

The results of the study obtained that: First Prevention of cyberbullying crimes as a whole can not be achieved by the current criminal law. Although there has been an ITE Act, but in its implementation many obstacles faced by law enforcement. This is because there are some limitations of criminal law to prevent cyberbullying crime. With regard to some of these limitations, the policy of applying criminal law needs to be balanced with nonpenal policy. Even non penal policies have a very strategic role in the prevention of cyberbullying crime. Second, cyberbullying prevention formulation is based on the effort to eliminate the causes and conditions that give rise to the crime. In synergizing penal and non penal policies, there needs to be a policy-oriented approach. The main problem in integrating and harmonizing penal policies with non-identifyers towards the emphasis and reduction of potential factors that foster crime. Through the intergral approach, it is hoped that the implementation of the social protection plan will be successful. Such success can sustain the achievement of the social policy objectives set forth in the national development plan.

Based on the results of this study the authors provide suggestions, among others: First, the criminal law still has limitations to combat cyberbullying crime, therefore countermeasures are not only done by applying the Act only. Supposedly, non-penal prevention efforts with emphasis on education to the public about the code of ethics using social networking. In addition, it should be prevention in the field of technology as well by increasing the security of information systems. Secondly, should be discussed soon and made a regulation on Crime in Information Technology because this bill can be complementary to UU ITE to further improve criminal law capability in eradicating cyberbullying crime in Indonesia.

DAFTAR ISI

DAFTAR LAMPIRAN

BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi memegang peranan yang sangat penting.[1]. Perkembangan teknologi informasi yang semakin pesat mampu mengubah pola kehidupan masyarakat dalam hal pemenuhan informasi. Sebagai akibat dari perkembangan tersebut, maka lambat laun teknologi informasi dengan sendirinya mengubah perilaku masyarakat dan peradaban manusia secara global. Munculnya *internet* merupakan salah satu penemuan yang berharga, karena dengan menggunakan internet kita bisa mendapatkan informasi-informasi yang dibutuhkan, dan seseorang dapat berkomunikasi dengan menggunakan *internet* walaupun jaraknya jauh. Seiring berjalannya waktu, akses internet menjadi semakin mudah. Segala bentuk informasi dapat menyebar secara cepat bahkan sulit untuk dikontrol.

Teknologi informasi dan media elektronika dinilai sebagai simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial budaya, ekonomi dan keuangan. Dari sistem-sistem kecil lokal dan nasional, proses globalisasi dalam tahun-tahun terakhir bergerak cepat, bahkan terlalu cepat menuju suatu sistem global.[2]

---

[1] Agus Rahardjo. 2002. *Cybercrime-Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung : Citra Aditya Bakti, halaman 1

[2] Didik J.Rachbini. 2001. *"Mitos dan Implikasi Globalisasi"* : Catatan Untuk Bidang Ekonomi dan Keuangan, Pengantar edisi Indonesia dalam Hirst, Paul dan Grahame Thompson, Globalisasi adalah Mitos, Jakarta : Yayasan Obor, halaman 2.

Sebagaimana ditulis dalam *International Review of Law Computer and Technology* :[3]

> *Global information and communication networks are now an integral part of the way in which modern governments, businesses, education and ecomomies operate. However, the increasing dependence upon the new information and communication technologies by many organizations is not without its price, they have become more exposed and vulnerable to an expanding array of computer security risks or harm and inevitably to various kinds of computer misuse.* (Informasi dan komunikasi global jaringan sekarang merupakan bagian integral dari cara dimana pemerintah modern, bisnis, pendidikan dan ekonnomi beroperasi. Namun, meningkatkan ketergantungan pada informasi dan komunikasi teknologi baru oleh banyak organisasi bukan tanpa harga, mereka hanya telah menjadi lebih terbuka dan rentan terhadap aturan memperluas risiko keamanan komputer atau bahaya dan pasti untuk berbagai jenis penyalahgunaan komputer)

Proses globalisasi tersebut melahirkan suatu fenomena yang mengubah model komunikasi konvensional dengan melahirkan kenyataan dalam dunia maya (*virtual reality*) yang dikenal sekarang ini dengan internet. Internet berkembang demikian pesat sebagai kultur masyarakat modern, dikatakan sebagai kultur karena melalui internet berbagai aktifitas masyarakat *cyber* seperti berpikir, berkreasi, dan bertindak dapat diekspresikan di dalamnya, kapanpun dan dimanapun. Kehadirannya telah membentuk dunia tersendiri yang dikenal dengan dunia maya (*Cyberspace*) atau dunia semu yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk *virtual* (tidak langsung dan tidak nyata).[4]

Pengguna *internet* di Indonesia dari tahun ke tahun semakin meningkat. Data yang diperoleh dari *Internet World Statistics* menunjukkan jumlah pengguna

---

[3] *International Review of law Computers and Technology, 'Insider Cyber-Threat: Problems and Perspectives'*.2001. Volume 14, Pages 105-113

[4] Agus Rahardjo, *Op.Cit*., halaman 20

internet di Indonesia pada tahun 2016 sudah mencapai 132 juta orang dan menduduki peringkat ketiga terbanyak di Asia setelah China dan India. Sedangkan menurut survey dari *We Are Social* data pengguna internet di Indonesia pada Januari 2016 mencapai 88,1 Juta dengan 79 juta di antaranya merupakan pengguna media sosial aktif, 15% nya pengguna aktif *facebook* dan hampir 50%. penggunanya adalah remaja berusia 13-29 tahun.[5]

Kemajuan teknologi informasi khususnya media *internet*, dirasakan banyak memberikan manfaat seperti dari segi keamanan, kenyamanan dan kecepatan. Contoh sederhana, dengan dipergunakan internet sebagai sarana pendukung dalam pemesanan/reservasi tiket (pesawat dan kereta api), hotel, pembayaran tagihan telepon,listrik, telah membuat konsumen semakin nyaman dan aman dalam menjalankan aktivitasnya. Kecepatan melakukan transaksi perbankan melalui *e-banking*, memanfaatkan *e-commerce* untuk mempermudah melakukan pembelian dan penjualan suatu barang serta menggunakan *e-library* dan *e-learning* untuk mencari referensi atau informasi ilmu pengetahuan yang dilakukan secara *on line* karena dijembatani oleh teknologi internet baik melalui komputer atau pun *hand phone. Internet* dapat memudahkan penggunannya untuk bertukar informasi tanpa harus bertatap muka satu sama lain. Selain itu adanya *internet* juga mendorong munculnya berbagai media sosial seperti *facebook, twitter, instagram* dan sebagainya

Pemanfaatan teknologi *internet* juga tidak dapat dipungkiri membawa dampak negatif yang tidak kalah banyak dengan manfaat positif yang ada.

[5] http://www.internetworldstats.com/stats3.htm Diakses 19 November 2016

Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian, pencemaran nama baik, pornografi, perjudian, penipuan hingga tindak pidana terorisme kini melalui media *internet* beberapa jenis tindak pidana tersebut dapat dilakukan secara *on line* oleh individu maupun kelompok dengan resiko tertangkap yang sangat kecil dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara.[6]

Berdasarkan data dari *Clear Commerce* tahun 2002 Indonesia diposisikan sebagai negara asal *carder* terbanyak ke dua di dunia setelah Ukraina. Menurut Anton Taba, Staf Ahli Kapolri, pada tahun 2009, Indonesia sudah menduduki peringkat pertama sebagai negara asal *carder,* dan pada tahun 2011, Indonesia menduduki peringkat 11 sebagai negara yang paling banyak melakukan pembajakan hak cipta. Faktanya, jumlah *cybercrime* di Indonesia justru makin meningkat setelah pemberlakuan UU No. 19 tahun 2016 perubahan atas UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai salah satu dasar hukum untuk mengadili perkara *cybercrime* di Indonesia.[7]

Perkembangan yang pesat dalam teknologi internet menyebabkan kejahatan-kejahatan di bidang teknologi informasi atau dapat disebut *cybercrime* atau *computer-related crime* yang semakin marak di Indonesia. *Cybercrime* adalah aktivitas manusia di dunia mayantara (maya) yang menjadikan komputer sebagai sasaran kejahatan (misalnya akses ilegal, perusakan situs, intersepsi

---

[6] Petrus Reinhard Golose, *Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia Oleh Polri*, Makalah pada Seminar Nasional tentang "Penanganan Masalah *Cybercrime* di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh Terpadu", diselenggarakan oleh Deplu,BI, dan DEPKOMINFO, Jakarta, 10 Agustus 2006, halaman 5.

[7] Widodo. 2011. *Aspek Hukum Pidana Kejahatan Mayantara,* Yogyakarta : Aswaja Pressindo, halaman v

ilegal), dan aktivitas manusia yang menggunakan komputer sebagai sasaran kejahatan (misalnya pemalsuan kartu kredit, pornografi *via* internet).[8]

Salah satu kejahatan di dunia mayantara yakni *Cyberbullying* yang merupakan bentuk intimidasi yang dilakukan seseorang atau lebih untuk memojokkan, menyudutkan, orang lain melalui dunia *cyber*. Pengertian *cyberbullying* adalah penggunaan teknologi *internet* untuk menyakiti orang lain dengan cara sengaja dan diulang-ulang". Intimidasi ini tidak sembarangan akibatnya, tak jarang kematian menjadi akhir dari *cyberbullying*. *Cyberbullying* juga diartikan sebagai bentuk intimidasi yang pelaku lakukan untuk melecehkan korbannya melalui perangkat teknologi. Pelaku ingin melihat seseorang terluka, ada banyak cara yang mereka lakukan untuk menyerang korban dengan pesan kejam dan gambar yang mengganggu dan disebarkan untuk mempermalukan korban bagi orang lain yang melihatnya.

Pada kenyataanya terdapat banyak kasus baik diluar negeri maupun di Indonesia yang menyangkut tentang *Cyberbullying*. Diantaranya kasus *Cyberbullying* yang terjadi di Indonesia dan masih terbilang baru adalah kasus Sonya Depari. Dia adalah seorang siswa Sekolah Menengah Atas (SMA) Methodist 1 Medan mengaku sebagai anak Arman Depari ketika di razia oleh polisi saat merayakan hari terakhir Ujian Nasional Rabu (6/4/2016). Pada saat hal itu terjadi, ada seseorang yang merekam dan kemudian video Sonya Depari tersebut menjadi viral. Setelah kejadian tersebut, Sonya Depari mendapat banyak cacian dari *netizen.*

[8] *Ibid*

Adapun kasus *cyberbullying* yang dialami Afi baru-baru ini. Tulisan Afi yang dituding hasil plagiarisme berjudul "Belas Kasih dalam Agama Kita". Dalam tulisan yang diberi tanda hak paten atas namanya itu dianggap bukan karya asli remaja 18 tahun tersebut, lantaran memiliki kesamaan dengan tulisan milik Mita Handayani yang berjudul "Agama Kasih". Mita mempublikasikan tulisannya itu pada 30 Juni 2016. Tudingan itu bermula dari tulisan seorang *netizen* bernama Pringadi Abdi Surya di *blog* Kompasiana, pada Rabu, 31 Mei 2017. Tulisan berjudul "Drama 'Dugaan' Plagiarisme Afi Nihaya Fardisa", Pringadi menilai tulisan Afi lainnya, seperti "Warisan" juga ditengarai memiliki roh yang sama dengan narasi sebuah video viral yang diterjemahkan Mita.

Afi mulai dikenal setelah tulisannya berjudul "Warisan" menghebohkan dunia maya. Asa Firda Inayah atau Afi, remaja asal Banyuwangi yang statusnya viral di media sosial mengaku depresi dan sempat berpikir untuk bunuh diri ketika dia di- *bully* di media sosial karena dugaan plagiat yang menimpanya.Bahkan walaupun dia sudah meminta maaf dan mengaku kesalahannya, hujatan kepada dia tidak pernah berhenti baik melalui kolom komentar statusnya, pesan masuk di media sosialnya dan di telepon selulernya sehingga dia pun mengganti nomor telepon. [9]

Karakteristik aktivitas di dunia *cyber* yang bersifat lintas batas yang tidak lagi tunduk pada batasan-batasan teritorial dan hukum tradisional memerlukan hukum responsif sebab pasal-pasal tertentu dalam KUHP dianggap tidak cukup

[9] http://regional.kompas.com/read/2017/06/15/10434431/afi.di-.bully.orang.se-indonesia.itu.tidak.mudah diakses 15 Juni 2017, pukul 00.36 WIB

memadai untuk menjawab persoalan-persoalan hukum yang muncul akibat aktivitas di dunia *cyber*. Pasal dalam KUHP yang relevan terhadap *cyberbullying* adalah Pasal 310 dan Pasal 311 KUHP.

Dalam UU No. 19 tahun 2016 perubahan atas UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) terdapat macam-macam jenis *Cybercrime* yang diatur dalam BAB VII tentang perbuatan yang dilarang. *Cyberbullying* termasuk dalam perbuatan yang dilarang yang diatur dalam Pasal 27 ayat (3) " Setiap orang sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat di aksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik". Kemudian Pasal 27 ayat (4) "Setiap orang sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat di aksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman. UU ITE hanya memuat unsur penghinaan dan pengancaman, padahal tindakan *cyberbullying* lainnya juga kerap kali terjadi dan menjadi awal tindak pidana lain. Dengan berkembangnya situs jejaring sosial maka hal tersebut akan memudahkan pelaku *cyberbullying* melakukan tindakannya.

Kriminalisasi terhadap perbuatan dunia mayantara muncul ketika dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakat yang sebelumnya belum diatur oleh hukum pidana. Hukum selalu berkembang dan semakin diperluas untuk mencakup situasi atau perubahan teknologi informasi yang terus berkembang dalam kehidupan masyarakat, perubahan hukum

akan menuntut masyarakat dunia maya untuk menyesuaikan dengan hukum yang baru tersebut. Akan tetapi pada kenyataannya hukum sendiri belum dapat mengatasi secara riil terhadap permasalahan-permasalahan yang ditimbulkan oleh teknologi khususnya teknologi informasi. Salah satu bukti konkretnya adalah timbulnya berbagai kejahatan di dunia virtual yang ternyata belum bisa diatasi sepenuhnya oleh hukum. Hukum pidana yang berlaku di Indonesia belum cukup untuk menyelesaikan kasus *Cyberbullying* yang terjadi di Indonesia.

Dalam perspektif lain, dalam pasal 3 UU ITE, teknologi informasi menjadi mungkin dalam formatnya saat ini karena difasilitasi oleh komputer yang didalamnya terdapat dua komponen pokok yaitu perangkat keras (*hardware*) dan perangkat lunak *(software)*. Wujud *hardware* berupa antara lain tidak terbatas pada : personal komputer,komputer mini dan *mainframe, note book, palmtop*, printer, modem, dan lain sebagainya. Adapun *software* antara lain terdiri dari kelompok: sistem operasi, *data base*, sistem aplikasi, dan bahasa pemrogaman (*progamming language*).

Hal ini dikarenakan hukum pidana hanya menormakan yang berisi larangan dan ancaman. Sehingga dibutuhkan disiplin ilmu lain, untuk menyelesaikan kasus kejahatan *cyberbullying* yaitu pencegahan di bidang tekhnologi (*Technology Prevention*). *Technology Prevention* merupakan upaya non penal hukum pidana untuk mencegah terjadinya *cyberbullying* di Indonesia dengan menggunakan pendekatan teknologi.

Pendekatan teknologi ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari

kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau *cultural* ini perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan.

Berdasarkan uraian di atas, penulis tertarik mengkaji lebih mendalalam tentang pencegahan kejahatan *Cyberbullying* dengan memanfaatkn teknologi informasi tersebut sebagai kajian dalam penulisan tesis yang berjudul "**KEBIJAKAN INTEGRAL HUKUM PIDANA DENGAN *TECHNOLOGY PREVENTION* DALAM UPAYA PENCEGAHAN KEJAHATAN *CYBERBULLYING*".**

1.2. Rumusan Masalah

1. Apakah dalam mencegah kejahatan *cyberbullying* akan dapat dicapai dengan menggunakan hukum pidana?
2. Bagaimana formulasi kebijakan integral hukum pidana dengan menggunakan sarana *Techno Prevention* sebagai upaya pencegahan kejahatan *cyberbullying* di masa yang akan datang?

1.3. Tujuan Penelitian

Menurut Bruggink, tujuan penelitian adalah hal penentuan tujuan (*doelstelling*) atau kepentingan pengetahuan (*kennisbelang*).[10] Tujuan yang hendak dicapai dalam penyusunan tesis hukum sebagaimana dirumuskan dalam rumusan masalah sebagaimana telah disebutkan, meliputi 2 (dua) hal, yaitu:

[10] J.J.H Bruggink, Alih Bahasa Arief Sidharta. 1996. *Refleksi tentang Hukum*, Bandung: Citra Aditya Bakti, halaman 216

1. Mengetahui dan memahami apakah kejahatan *cyberbullying* akan dapat dicapai dengan menggunakan hukum pidana;
2. Mengetahui dan meamahami formulasi kebijakan integral hukum pidana dengan menggunakan sarana *Techno Prevention* sebagai upaya pencegahan kejahatan *cyberbullying* di masa yang akan datang.

1.4. Manfaat Penelitian

1. Secara teoritis sebagai sarana pengembangan ilmu pengetahuan bidang hukum tentang hukum pidana;
2. Secara praktis sebagai pedoman bagi masyarakat untuk lebih memahami tentang hukum pidana.

1.5. Originalitas Penulisan

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

1. Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi melalui Hukum Pidana, pada program magister ilmu hukum Universitas Diponegoro Semarang tahun 2008 oleh Philemon Ginting, SIK. Dalam penelitian tersebut dibahas kriminalisasi terhadap perbuatan dunia mayantara muncul ketika dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakat yang sebelumnya belum diatur oleh hukum pidana. Hukum selalu berkembang dan semakin diperluas untuk mencakup situasi atau perubahan teknologi

informasi yang terus berkembang dalam kehidupan masyarakat, perubahan hukum akan menuntut masyarakat dunia maya untuk menyesuaikan dengan hukum yang baru tersebut. Akan tetapi pada kenyataannya hukum sendiri belum dapat mengatasi secara riil terhadap permasalahan-permasalahan yang ditimbulkan oleh teknologi khususnya teknologi informasi. Salah satu bukti konkretnya adalah timbulnya berbagai kejahatan di dunia virtual yang ternyata belum bisa diatasi sepenuhnya oleh hukum.

2. Kebijakan Kriminal terhadap *Cyber Terorism* di Indonesia, pada program magister ilmu hukum Universitas Diponegoro Semarang tahun 2009 oleh Nanda Ivan Natzir. Dalam penelitian tersebut dibahas proteksi terhadap *netizen/netter* (warga dunia maya-pengguna jasa internet) dari tindak kejahatan *cyber*, selain melalui perangkat teknologi dan berbagai pendekatan lain tersebut juga melalui sarana hukum, khususnya *cyber crime law* (hukum pidana siber). Namun membuat suatu ketentuan hukum terhadap bidang yang berubah cepat sungguh bukanlah suatu hal yang mudah, karena disini lah terkadang hukum (peraturan perundang-undangan) tampak cepat menjadi usang manakala mengatur bidang-bidang yang mengalami perubahan cepat, sehingga situasinya seperti terjadi kekosongan hukum (*vaccum rechts*). Di sisi lain, banyak negara yang telah melakukan pengembangan sistem hukum nasionalnya untuk menyikapi dan mengakomodir perkembangan internet, khususnya dengan membuat produk-produk legislatif yang baru yang berkaitan dengan keberadaan internet.

Berdasarkan kedua rujukan penelitian yang pernah dilakukan sebelumnya, penulis dalam penulisan tesis ini akan mengkaji suatu permasalahan hukum dimana penelitian ini berbeda dengan penelitian tersebut dengan berangkat dari pemikiran sebagaimana telah diuraikan dalam latar belakang di atas, dalam penelitian pertama, dalam penelitian tersebut dibahas bahwa kebijakan formulasi tindak pidana teknologi informasi (UU ITE) harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidanaan umum yang berlaku saat ini. Tidaklah dapat dikatakan harmonisasi/sinkronisasi apabila kebijakan formulasi berada diluar sistem. Oleh karena itu kebijakan formulasi hukum pidana tindak pidana teknologi informasi harus berada dalam sistem hukum pidana yang berlaku saat ini.

Dalam penelitian kedua Kebijakan non penal/*non penal policy* dapat dilakukan dengan meningkatkan peran serta penggunaan alat dan teknologi modern yang berfungsi sebagai penyaring atau filter yang umumnya berupa *software protection*, karena kebijakan penanggulangan bisa diterima jika dikombinasikan dengan menyaring perangkat lunaknya. Dari sudut pendekatan teknologi (*techno prevention*), guna mengatasi penyalahgunaan pemakain internet oleh para kaum hacker dan cracker/ *Cyber Terorism*, maka perlu dapat ditingkatkan sistem pengaman pada sistem komputer dan jaringan internet.

Penulis dalam melakukan penulisan penelitian ini berorientasi pada pencegahan kejahatan *cyberbullying* menggunakan pendekatan menggunakan *Techno Prevention* atau pendekatan di bidang teknologi. Hak ini dikarenakan kejahatan di bidang *cyber* ini mempunyai dampak yang serius untuk

perkembangan pola pikir masyarakat Indonesia khususnya remaja Indonesia. Remaja Indonesia yang sangat erat kaitannya dengan *gadget* yang mengakibatkan ketergantungan terhadap internet sehingga dengan mudah dapat mengakses segalanya melalui internet. Tak jarang jika penggunaan internet ini dapat digunakan sebagai sarana kejahatan seperti kekerasan atau intimidasi menggunakan jaringan komputer tersebut. Dalam penelitian tersebut, penulis juga berharap kejahatan *cyberbullying* ini dapat diatur keberadaannya mulai dari unsur-unsur dan penjatuhan sanksi pidana.

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.[11] 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 pembatasan-pembatasan tertentu untuk menghindari jalan yang menyesatkan dan tidak terkendalikan.[12]

---

[11] Ronny Hanitijo Soemitro. 1988. *Metode Penelitian Hukum dan Jurimetri*, Jakarta: Rinneka Cipta, halaman 10

[12] Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*. 2006. Edisi Revisi, Cetakan II, Malang : Banyumedia Publishing halaman294

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.[13]

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. Hasil dari telaah tersebut merupakan suatu argumen untuk memecahkan isu yang dihadapi [14]
2. Pendekatan Konseptual (*Conseptual Approach*), metode pendekatan dengan merujuk pada prinsip-prinsip hukum, yang dapat diketemukan dalam pandangan-pandangan sarjana ataupun doktrin-doktrin hukum.[15]
3. Pendekatan Historis (*Hystorical Approach*), dilakukan dengan menelaah latar belakang apa yang dipelajari dan perkembangan pengaturan mengenai isu yangv dihadapi. Telaah demikian diperlukan oleh peneliti memang ingin

---

[13] Peter Mahmud Marzuki. 2013. *Penelitian Hukum*, Jakarta : Kencana Media Group, halaman 194

[14] Peter Mahmud Marzuki. 2014 *Penelitian Hukum*. Jakarta : Kencana Prenada Media Group, halaman 93

[15] *Ibid*, halaman 138

mengungkap filosofis dan pola pikir yang melahirkan sesuatu yang sedang dopelajari.[16]

1.6.3 Sumber Bahan Hukum

Bahan hukum merupakan sarana dari suatu penelitian yang dipergunakan untuk memecahkan masalah yang ada. Bahan hukum yang diperoleh terdiri dari bahan hukum primer dan sekunder.[17]

1) Bahan Hukum Primer

Bahan hukum primer ini dalam hal ini berupa peraturan dasar, peraturan perundang-undangan, dan norma hukum. Bahan hukum primer dalam penulisan tesis hukum ini, meliputi :

1. Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Kitab Undang-Undang Hukum Pidana;
2. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana;
3. Undang-Undang Nomor 19 tahun 2016 perubahan atas UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Selain itu dipergunakan pula beberapa ketentuan perundang-undangan atau peraturan lainnya yang terkait serta semua peraturan perundang-undangan lainnya yang berkaitan dengan permasalahan yang akan dikaji. Bahan hukum primer tersebut kemudian dianalisis, dikembangkan, dibandingkan, dan diuji untuk memperoleh kebenaran pengetahuan secara teoritis dan ilmiah.

[16] *Ibid*, halaman 138
[17] *Ibid*, halaman 155

Kesemuanya itu kemudian dihubungkan dan digunakan untuk mengembangkan jawaban dalam pokok permasalahan penyusunan tesis 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 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 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 menarik 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, atau menunjukkan komparasi atau hubungan seperangkat data dengan seperangkat data yang lain dengan sistematis berdasarkan kumpulan bahan hukum yang diperoleh, ditambahkan pendapat para sarjana yang mempunyai hubungan dengan bahan kajian sebagai bahan komparatif. Langkah-langkah selanjutnya yang dipergunakan dalam melakukan suatu penelitian hukum, yaitu : [18]

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

[18] *Ibid*, hlm.171

Langkah-langkah ini sesuai dengan karakter ilmu hukum sebagai ilmu yang bersifat preskriptif dan terapan. Sebagai ilmu yang bersifat preskripsi, 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 maupun yang untuk kajian akademis.

BAB 2

TINJAUAN PUSTAKA

2.1. Tinjauan tentang *Cybercrime*

2.1.1. Konsep *Cybercrime*

Kejahatan yang terjadi di dunia maya dengan menjadikan komputer sebagai sasaran atau komputer sebagai alat melakukan kejahatan lazim tersebut lazim dinamakan *computer-related crime.* Istilah ini seringkali digunakan oleh Perserikatan Bangsa – Bangsa (PBB), namun PBB kadang juga menggunakan *cybercrime* untuk menyebut kejahatan yang terjadi di dunia mayantara.[19] Menurut Kepolisian Ingris, *Cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan criminal dan/atau criminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.[20]

Pengertian computer dalam The Proposed West Virginia Computer Crimes Act adalah *"an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or type-setter, a portable hand-held calculator, or other similar device*". Dari pengertian kejahatan computer menurut peraturan perundang-undangan di Virginia dapat dipahami bahwa sesuatu yang

[19] Widodo, *Op. Cit*, halaman 5

[20] Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara* (*Cyber Crime*), Jakarta: PT. Refika Aditama, halaman 40

berhubungan dengan peralatan pemerosesan data listrik, magnetic, optic, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melalukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau tipe-setter, sebuah kalkulator tangan atau peralatan serupa lainnya.[21]

Di lihat dari beberapa definisi di atas, tampak bahwa belum ada kesepakatan mengenai definisi tentang cyber crime atau kejahatan dunia cyber. Menurut Muladi, sampai saat ini belum ada definisi yang seragam tentang cyber crime baik nasional maupun global. Kebanyakan masih menggunakan soft law berbentuk code of conduct seperti Jepang dan Singapura.[22]

Hal yang sama juga diungkapkan oleh Agus Raharjo bahwa istilah *cyber crime* sampai saat ini belum ada kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cyber crime* dengan *computer crime.*[23]

Berdasarkan modus operandinya, *cyber crime* terdiri dari dua jenis kejahatan, yaitu :[24]

---

[21] Abdul Wahid dan Mohammad Labib, *Op Cit.* halaman 41

[22] Suara Merdeka, 24 Juli 2002, situs internet: http://www.suaramerdeka.com/harian/0207/24/nas13.htm.

[23] Agus Raharjo. 2002. *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*,(Bandung :Citra Aditya Bhakti, halaman 227

[24] Dikutip oleh Tim Peneliti, *Tindak Pidana Teknologi Komunikasi Informasi/cyber crime danUpaya Penaggulangannya* (Laporan hasil Penelitian), Penelitian Dan Pengembangan IlmuPengetahuan Dan Tehnologi Kepolisian Perguruan Tinggi Ilmu Kepolisian (PPITK-PTIK),Jakarta, Desember, 2003, halaman 41, Dalam Dikdik M. Arief Mansyur dan Elisatris Gultom, *Cyber Law aspek hukum Teknologi Informasi*, 2005, (Refika Aditama;Bandung), halaman 87

a. Kejahatan yang sasaran/targetnya adalah fasilitas serta sistem teknologi komunikasi informasi. Para pelaku menggunakan sarana ini untuk menyerang atau merusak sarana teknologi informasi lainnya yang menjadi target. Pada posisi ini komputer/internet adalah alat sekaligus korban kejahatan. Kejahatan ini lebih dikenal *Hacking/cracking* yang menyerang program-program operasi jaringan komputer. Ini mempunyai sifat sebagai kejahatan baru (*new category of crime*).
b. Kejahatan umum/biasa yang difasilitasi oleh tekhnologi komunikasi informasi. Jenis kejahatan ini telah ada sebelum teknologi informasi bergerak menuju kearah penyalahgunaannya, contohnya penipuan kartu kredit, pengancaman, pencemaran nama baik, terorisme, pornografi dan sebagainya. Ini merupakan kejahatan yang bersifat biasa *(Ordinary crime)* yang pengaturannya telah terdapat dalam KUHP

1.1.2. Karakteristik dan Jenis *Cybercrime*

Berdasarkan literatur, *cybercrime* memiliki beberapa karakteristik, yaitu :[25]

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;

[25] Abdul Wahid dan M. Labib, *Op. Cit.* halaman 76

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*.

Karakteristik yang disebutkan oleh Abdul Wahid dan M. Labib di atas sejatinya hanya memberikan pembeda antara kejahatan tradisonal dengan *cybercrime* dalam ruang yang berbeda dan yurisdiksi. Sejatinya *cybercrime* muncul akibat kemajuan teknologi informasi dan digital, yang memudahkan orang-orang untuk melakukan komunikasi, mendapatkan informasi serta memudahkan bisnis. Disini lain, kemudahan yang diberikan oleh teknologi, menjadikan teknologi sebagai target untuk memperoleh dan menyebarkan gangguan. Dengan demikian, karakteristik dari *cybercrime* adalah penggunaan/pemanfaatan teknologi informasi/digital untuk melakukan kejahatan dan kejahatan yang didukung oleh teknologi informasi/digital.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain :[26]

1. *Unauthorized acces to computer system and service*, yaitu kejahakatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan

[26] Ari Juliano Gema, 2000, *Cyber Crime : Sebuah Fenomena di Dunia Maya".* www.thecelli.com diakses 29 Desember 2016

maksud sabotase ataupun pencurian informasi penting dan rahasia. Ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliaanya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.

2. *Illegal Contents,* yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum.
3. *Data Forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukkan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.
4. *Cyber Espionage,* yaitu kejahatan yang memanfaatkan teknologi internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi .
5. *Cyber Sabotage and extortion,* yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb,* virus komputer ataupun suatu program tertentu sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan

sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6. *Offence against intellectual property,* yaitu kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet.
7. *Infringements of privacy*, yaitu kejahatan yang ditujujan terhadap informai seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujkan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara materiil maupun immateriil seperti nomor kartu kredit, nomor pin ATM, keterangan tentang cacat atau penyakit tersembunyi, dsb.

Satu-satunya instrumen internasional yang mengatur kejahatan yang berhubungan dengan komputer adalah *Convention on Cybercrime*. Dalam Bab II Konvensi tersebut diatur tentang hukum pidana substantif, yaitu sebagaimana terjabar dalam Pasal (*article*) 2 sampai dengan Pasal 11. Sedangkan Psal 12-13 mengatur mengenai ketentuan pemidanaan. Ketentuan tersebut sebagaiman berikut:[27]

> *2. Title 1, offense against the confidentiality, integrity and availability of computer data and system.*
> *a. illegal acces*
> *b. illegal interception*
> *c. data inteference*
> *d. damaging, deletion, deteriotartion, alteration or suppression of computer data without right (article 4);*
> *e. system interference (article 5);*
> *f. misuse of devices (acces code) (article 6).*
> *3. Title 2, Computer Related Offences:*

[27] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara* , Op.Cit. halaman 61

a. Computerrelated forgery (article 7);
b. Computer related fraud (article 8).
1. Title 3, Content Related Offences
2. Title 4, Offences Related to Infringement of Copyright and Related Right (article 10)...
3. Title 5, anciallary laibility and sanction (article 11; (article 12), (article 13)

Berdasarkan ringkasan ketentuan dalam *Convention on Cybercrime* dapat dipahami bahwa dalam bagian 1. Pelanggaran terhadap kerahasiaan, ketersediaan dan intergritas sistem dan data computer, terdiri atas perbuatan berikut :[28]

a. Akses tidak sah, yaitu sengaja memasuki/mengakses komputer tanpa hak (Pasal 2)
b. Intersepsi tidak sah, yaitu sengaja dan tanpa hak mendengar / mengkap secara diam-diam pengiriman transmisi dan pemancaran (emisi) data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis (Pasal 3);
c. Gangguan/perusakan data, yaitu sengaja dan tanpa hak melakukan perusakan;
d. Penghapusan, perubahan atau penghapusan data komputer (Pasal 4);
e. Gangguan/perusakan sistem, yaitu sengaja melakukan gangguan/rintangan secara serius tanpa hak terahadap berfungsinya sistem komputer (Pasal 5);
f. Penyalahgunaan peralatan, yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, *password* komputer, kode masuk (*acces code*) (Pasal 6).

Kemudian dalam bagian 2, diatur tentang pelanggaran yang berhubungan dengan komputer, yaitu dalam bentuk berikut :[29]

[28] *Ibid,* halaman 62

a. Pemalsuan yang berhubungan dengan komputer (Pasal 7): Pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data otentik menjadi tidak otentik dengan meksud untuk digunakan sebagai data otentik)
b. Penipuan yang berhubungan dengan komputer (Pasal 8), yaitu penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain)

Selanjutnya dalam bagian 3 tentang Pelanggaran yang berhubungan dengan isi, yaitu berkaitan dengan delik-delik yang berhubungan dengan pornografi anak (Pasal 9), yaitu meliputi perbuatan: [30]

a. Memproduksi dengan tujuan mendistribusikan melalui sistem komputer;
b. Menawarkan melalui sistem komputer;
c. Mendistribusikan atau mengirim melalui sistem komputer;
d. Memperoleh melalui sistem komputer;
e. Memiliki dalam sistem komputer atau di dalam media penyimpan data.

Akhirnya dalam bagian 4 tentang pelanggaran yang berhubungan dengan Hak Cipta (Pasal 10), yaitu delik-delik yang terkait dengan pelanggaran hak cipta. Sedangkan pada bagian 5, diatur tentang pertanggungjawaban pidana dan sanksi; Percobaan dan Pembantuan (Pasal 11); Pertanggungjawaban Korporasi (Pasal 12); Sanksi dan tindakan (Pasal 13).[31]

---

[29] *Ibid*
[30] *Ibid*
[31] *Ibid,* halaman 63

2.1.3 Pengaturan *Cybercrime* di Indonesia

UU ITE yang diundangkan di Jakarta pada tanggal 21 April 2008 dan dicatat dalam Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58 merupakam jawaban pemerintah Indonesia untuk menanggulangi *cybercrime*. Namun bukan Undang-Undang yang pertama kali di Indonesia yang dapat menjangkau *cybercrime*, karena jauh sebelum Undang-Undang ini disahkan, penegak hukum menggunakan KUHP dan beberapa aturan diluar KUHP untuk mengadili *cybercrime*.

Ketentuan dalam KUHP yang dapat digunakan untuk menjerat pelaku *cybercrime* dengan menggunakan penafsiran ekstensif diantaranya adalah ketentuan tindak pidana pemalsuan (Pasal 263 sampai Pasal 276), tindak pidana pencurian (Pasal 362 sampai dengan Pasal 367), tindak pidana Penipuan (Pasal 378 sampai dengan Pasal 395), dan tindak pidana perungsakan barang (Pasal 406 sampai dengan Pasal 412).[32]

Selain penafsiran ekstensif terhadap Pasal-Pasal dalam KUHP, peraturan perundang-undangan di luar KUHP yang dapat digunakan sebagai dasar untuk mengadili *cybercrime* (dengan menggunakan penafsiran ekstensif) sebelum keluarnya Tentang ITE adalah:[33]

1. Undang-Undang No. 11/Pnps/1963 Tentang Pemberantasan Subversi (sudah dicabut);

---

[32] Aloysius Wisnubroto. 1999. *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer,* Yogyakarta : Universitas Atmajaya, halaman 115

[33] Muladi. 2002. *Demokrasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*, Jakarta : Habibie Center, halaman 217

2. Undang-Undang No. 3 Tahun 1971 Tentang Pemberantasan Tindak Pidana Korupsi, yang kemudian diganti dengan Undang- Undang No. 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi dan terakhir diubah dengan Undang-Undang No. 20 Tahun 2001 Tentang Perubahan No. 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi;
3. Undang-undang No. 10 Tahun 1995 Tentang Kepabeanan;
4. Undang-Undang No. 10 Tahun 1998 Tentang Perbankan;
5. Undang-Undang No. 36 Tahun 1999 Tentang Telekomunikasi;
6. Undang-Undang No. 15 Tahun 2002 Tentang Pencucian Uang;
7. Undang-Undang No. 19 Tahun 2002 Tentang Hak Cipta;
8. Undang-Undang No. 32 Tahun 2002 Tentang Penyiaran;
9. Undang-Undang No. 15 Tahun 2003 Tentang Pemberantasan Terorisme

Setelah lahirnya UU ITE sebagai *cyberlaw*, Indonesia mengkasifikasikan *cybercrime* dalam 7 (tujuh) kategori, yaitu:

1. *Illegal content*, meliputi;
   a. Konten yang melanggar kesusilaan (Pasal 27 ayat (1))
   b. Konten yang memiliki muatan perjudian (Pasal 27 ayat (2))
   c. Konten yang memiliki muatan penghinaan dan/atau pencamaran nama baik (Pasal 27 ayat (3))
   d. Menyebarkan berita bohong yang merugikan konsumen (Pasal 28 ayat (1))
   e. Menyebarkan informasi yang dapat menimbulkan rasa kebencian dan permusuhan (Pasal 28 ayat (2))

f. Konten yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29)

2. *Illegal access*, meliputi;

a. mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun (pasal 30 ayat (1))

b. mengakses Komputer dan/atau Sistem Elektronik dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik (Pasal 30 ayat 2))

c. mengakses Komputer dan/atau Sistem Elektronik dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (Pasal 30 ayat (3)

3. *Illegal interception*, meliputi;

a. melakukan penyadapan komputer/sistem elektronik milik orang lain (Pasal 31 ayat (1))

b. melakukan penyadapan informasi elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain (Pasal31 ayat (2))

4. *Data interference*, meliputi;

a. mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik (Pasal 32 ayat (1)

b. memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak (Pasal 32 ayat (2))

c. membuka informasi elektronik yang bersifat rahasia dan menjadi dapat diakses oleh publik (Pasal 32 ayta (3) 5. *System interference*, meliputi; melakukan tindakan apapun yang berakibat terganggunya sistem elektronik atau tidak bekerjanya sistem elektronik sebagaimana mestikanya (Pasal 33)

6. *Misuse of device*, meliputi;

a. menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki; perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33 (Pasal 34 ayat (1))

b. menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki; 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 (Pasal 34 ayat (1))

7. *Computer related forgery*, meliputi;

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 (Pasal 35)

Secara spesifik, terdapat perbedaan pengaturan tentang *cybercrime* antara UU ITE dengan hasil *Convention on Cybercrime*. Namun kelahiran UU ITE sebagai *cyberlaw* di Indonesia, perlu diapresiasi karena globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia, dengan adanya UU ITE sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa.

2.1. Tinjauan tentang *Cyberbullying*

2.2.1 Konsep *Cyberbullying*

Bullying dapat didefinisikan sebagai sebuah kegiatan atau perilaku agresif yang sengaja dilakukan oleh sekelompok orang atau seorang secara berulang-ulang dan dari waktu ke waktu terhadap seorang korban yang tidak dapat mempertahankan dirinya dengan mudah atau sebuah penyalahgunaan kekuasaan/kekuatan secara sistematik. Kriteria pengulangan, niat dan ketidakseimbangan kekuatan sistematik menjadikan *bullying* bentuk agresi yang sangat tidak diharapkan. Ini dapat terjadi di banyak konteks termasuk di tempat kerja, tetapi yang paling banyak diteliti adalah di remaja.[34]

Cyberbullying merupakan istilah yang ditambahkan ke dalam kamus OED pada tahun 2010. Istilah ini merujuk kepada penggunaan teknologi informasi

[34] Kathryn Gerald. 2012. *Intervensi Praktis Bagi Remaja Beresiko*. Yogyakarta: Pustaka Pelajar. halaman 72

untuk menggertak orang dengan mengirim atau *posting* teks yang bersifat mengintimidasi atau mengancam. OED menunjukkan penggunaan pertama dari istilah ini pertama kali di Canberra pada tahun 1998, tetapi istilah ini sudah ada sebelumnya di Artikel New Yorks Time 1995 di mana banyak sarjana dan penulis Besley seorang Kanada yang meluncurkan *website cyberbullying* tahun 2013 dengan istilah *coining*.[35]

Secara umum *cyber bullying* yaitu perlakuan kasar yang dilakukan oleh seseorang atau sekelompok orang, menggunakan bantuan alat elektronik yang dilakukan berulang dan terus menerus pada seorang target yang kesulitan membela diri. [36]

Cyber bullying merupakan aktivitas menggunakan teknologi informasi dan komunikasi secara disengaja, berulang-ulang dan terus-menerus mengandung permusuhan yang dilakukan oleh individu atau kelompok dengan tujuan untuk melukai perasaan orang lain (kelompok atau indvidu).

Dalam peraturan perundang-undangan, tindakan *cyber bullying* belum diatur dalam Undang-Undang yang khusus. Walaupun belum ada Undang - Undang yang secara khusus mengatur tentang tindakan *cyber bullying*, tetapi perbuatan yang termasuk dalam *cyber bullying* dapat diancam pidana melalui UU ITE. Pasal yang dapat dikenai dalam tindakan *cyber bullying* adalah Pasal 27 ayat

[35] Sheri Bauman, Donna Cross and Jenny Walker. 2013. *Principles of Cyberbullying* New York: Taylor ang Francis Group, halaman 23.

[36] http://mycyberbullying.wordpress.com/2014/05/25/pengertian-cyberbullying/, diakses pada Sabtu, 27 Januari 2017, pada pukul 19:40 WIB

(1), (3), dan (4); Pasal 28 ayat (2), dan Pasal 29. Dalam pasal-pasal tersebut, yang diatur adalah:

Pasal 27

(1) 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 yang melanggar kesusilaan.
(3) 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 penghinaan dan/atau pencemaran nama baik.
(4) 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 pemerasan dan/atau pengancaman.

Pasal 28

(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 antargolongan (SARA)

Pasal 29

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

2.2.2 Bentuk-bentuk *Cyberbullying*

a. *Flaming* (terbakar atau amarah) yaitu kegiatan *cyber bullying* berupa mengirimkan pesan yang berisi kata- kata amarah atau nafsu. Korban dalam aspek ini menerima pesan melalui *chat room* atau grup yang bernada amarah, kata-kata kasar, atau *vulgar*.
b. *Harassment* (pelecehan) yaitu kegiatan *cyberbullying* berupa mengirimkan pesan yang mengganggu secara berulang kali. Korban dalam aspek ini menerima pesan secara pribadi yang bermaksud menghina atau mengganggu secara berulang kali.

c. *Cyberstalking* (diikuti) yaitu kegiatan *cyberbullying* berupa mengikuti seseorang di dunia maya secara berulang kali.
d. *Denigration* (pencemaran nama baik) yaitu kegiatan *cyberbullying* dengan menyebarkan keburukan seseorang di dunia maya dengan maksud merusak reputasi orang tersebut.
e. *Impersonation* (peniruan) yaitu kegiatan *cyber bullying* dengan berpura-pura menjadi orang lain dan mengirimkan pesan yang tidak baik. Korban dalam aspek ini dijadikan terlihat buruk oleh pelaku yang berpura-pura menjadi korban.
f. *Outing* (menyebarkan rahasia pribadi) dan *trickery* (penipuan) adalah kegiatan *cyber bullying* berupa membujuk atau menipu seseorang untuk mengungkapkan rahasia pribadi lalu menyebarkannya.
g. *Exclusion* (pengeluaran) yaitu kegiatan *cyber bullying* berupa mengeluarkan seseorang secara kejam dan sengaja dari grup. Korban dalam aspek ini dikeluarkan dengan sengaja dari sebuah grup diskusi.

Beberapa bentuk *cyberbullying* yang telah dijelaskan, bahwa tindakan *cyberbullying* menitikberatkan kepada kekerasan secara verbal secara tidak langsung yang akan berdampak kepada kondisi emosional atau psikis dari korbannya. Dampak dari tindakan *cyberbullying* terhadap korbannya bermacam-macam, mulai dari timbulnya rasa tidak nyaman, ketakutan dalam hal kegiatan di

dalam dunia *cyber*, hingga yang paling parah melakukan perbuatan nekad seperti bunuh diri.[37]

Dalam penelitian yang dilakukan Price dan Dalgleish (2010) pada 548 remaja Australia dan juga didukung oleh penelitan-penelitian lainnya (Patchin, 2009) menggarisbawahi bentuk-bentuk *cyberbullying* yang dilakukan oleh pelaku remaja pada media internet. Bentuk-bentuk *cyberbullying* yang ditemukan antara lain;[38]

a. *Called Name* (Pemberian Nama Negatif)
   Pemberian nama negatif adalah bentuk serangan *cyberbullying* untukmemberi label buruk terhadap korban. Seorang pakar bullying, Sherry Gordon[39] mengemukakan pemberian nama negatif atau yang kerap disebut *name-calling* adalah salah satu bentuk *cyberbullying* yang palingmembahayakan. Pemberian nama negatif adalah berbahaya karena memaksa untuk mengecap seseorang yang bukan dirinya. Nama-nama negatif yang disebutkan dalam aksi *cyberbullying* terhadap korban antara lain; a) Nama hewan: tikus, beruk, monyet, anjing, babi b) Nama makhluk halus: kuntilanak, hantu c) Panggilan fisik: wajah, badan/keseluruhan fisik
b. *Image of Victim Spread* (Penyebaran Foto)
   Dalam ke empat kasus yang diteliti, diketahui pada tiap kasus pelaku menampilkan foto pribadi korban yang diunggah kedalam Facebook dandijadikan hinaan secara masif. *Image of victim spread* menurut Price dan Dalgleish (2010) adalah wujud dari ungkapan ekspresi pelaku untuk menghibur dirinya maupun orang lain dengan memakai foto korban sebagai objek hiburan. Namun, disisi lain Price dan Dalgeish juga mengutarakan bahwa penyebaran foto pribadi korban adalah aksi untuk membuat malu korban. Bentuk serangan *bullying* verbal dapat dilihat dari komentar yang ditulis pada tiap foto yang di tampilkan. Pada kasus Tiara, terlihat pelaku dengan sengaja mengedit foto Tiara dengan memperbesar area wajah dengan tujuan

---

[37] Kartika Risna. 2014. *Pencegahan Perilaku Bullying di Lingkungan*, Jakarta : Serambi, halaman 14

[38] Price, Megan & John Dalgleish, 2010, *Cyberbullying: Experiences, Impacts AndCoping Strategies As Described By Australian Young People*. Youth Studies Australia, v.29, n.2, halaman 45

[39] www.bullying.about.com, diakses 01 Juni 2017, pukul 05.24 WIB

untuk memalukan dan menghibur diri pelaku. Pada kasus selanjutnya, foto pribadi Safithree yang diunggah oleh Rizqita Ramadhani, Romi Marthin dan Cabe Rawit menjadi bahan ejekan dengan komentar yang ditambahkan pada foto tersebut. Foto pribadi Safithree tersebut dijadikan konsumsi publik dan dihina secara massif, sedangkan dalam kaidah sosial media foto pribadi seseorang adalah sebuah *privacy* yang harus dilindungi.

Dalam kasus Halida, Devy Ariani pengunggah foto Halida mengibaratkan pekerjaan yang sedang dilakukan Halida adalah layaknya seorang pelayan dengan memanggil dengan kata pelayan dan *mbok-mbok*. Dalam foto tersebut, Halida terlihat sedang menyetrika pakaian, namun karena komentar Devy yang mengkonotasikan seperti itu, Halida menjadi bahan bullying oleh teman-temannya pada komentar-komentar selanjutnya. Sementara pada kasus Ady, tampak foto yang diunggah oleh Nanang Pramono adalah foto Ady yang tidak mengenakan baju dan foto dia memakai seragam sekolah. Tampak normal pada kedua foto tersebut pada sosial media. Namun, teman-teman Ady menganggap foto tersebut adalah foto yang pas untuk di hina.

c. *Threatened Physical Harm* (Mengancam Keselamatan Fisik)
Cyberbullying juga dapat mengancam keselematan orang lain. Dalam hal ini, komentar-komentar yang berisi kata "mati" atau "bunuh" menjadi erat kaitannya dengan eksistensi keselataman orang lain pada dunia nyata. Salah satu contoh serangan *bullying* pada Facebook di kasus yang diteliti mengancam keselamatan adalah pada kasus Safitri. Dimana terdapat beberapa pelaku pembantu yang menuliskan kalimat ancaman yang dapat berpengaruh pada keselamatan Safitri.

d. *Opinion Slammed* (Pendapat Yang Merendahkan)
Opini merendahkan adalah pendapat yang ditulis pelaku kepada korban untuk menghina keadaan atau penampilan korban. Dalam pengamatan terhadap keseluruhan kasus, terdapat komentar-komentar yang bermuatan *cyberbullying* yaitu merendahkan korban. Komentar yang didapat dalam merendahkan seseorang terdapat pada kasus Halida dan Safithree. Halida di rendahkan pekerjaan yang dilakukan dan dianggap layaknya pembantu rumah tangga. Sedangkan Safithree dianggap seorang "Alay" atau anak kampong yang jauh dari kehidupan perkotaan yang tercukupi

2.2. Kebijakan Hukum Pidana

Istilah kebijakan berasal dari bahasa Inggris policy atau dalam bahasa Belanda politie. Black's Law Dictionary mengidentifikasikan Policy sebagai: *The*

general principles by which a government is guided in its management of public afairs, ...or principles and standard regarded by the ligislature or by the courts as being of fundamental concern to the state and the whole of society in measures, as applied to a law, ordinance, or rule of law, denotes its general purpose or tendency considered as directed to the welfare or prosperity of the state community.[40]

Istilah "*policy*" dalam bahasa Inggris atau "politiek" dalam bahas Belanda, kedua istilah asing ini, maka istilah "kebijakan hukum pidana" dapat pula disebut dengan istilah politik hukum pidana. Istilah politik hukum pidana ini, dalam kepustakaan asing sering dikenal dengan berbagai istilah antara lain "*penal policy*", "*criminal law policy*", atau "*strafrechtspolitiek*".[41]

Kebijakan kriminal dalam konteks ini dapat dimaknai sebagai upaya pemberantasan kejahatan, baik melalui kebijakan penal (pemberantasan kejahatan menggunakan hukum pidana) maupun kebijakan non penal (pemberantasan kejahatan) dengan tanpa menggunakan hukum pidana).[42]

Secara umum kebijakan dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah dalam mengelola, mengatur atau menyelesaikan urusan-urusan publik, masalah-masalah masyarakat atau bidang-bidang penyusunan peraturan perundang-undangan dan pengaplikasian

---

[40] Henry Campbell Black. 1999. "Black's Law Dictionary", Seventh Edition, St.Paulmin West Publicing,Co., halaman 117

[41] Barda Nawawi Arief. 1982. *Masalah Pemidanaan Sehubungan dengan Perkembangan Delik-delik Khusus Dalam Masyarakat Modern*, Bandung: Banacipta, halaman 22

[42] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara, , Op. Cit*., halaman 179

hukum/peraturan, dengan suatu tujuan yang mengarah pada upaya mewujudkan kesejahteraan atau kemakmuran masyarakat (warga negara).[43]

Dilihat sebagai bagian dari politik hukum maka politik hukum pidana mengandung arti, bagaimana mengusahakan atau membuat dan merumuskan suatu perundang-undangan pidana yang baik. Pengertian demikian terlihat pula dalam definisi penal policy dari Marc Ancel secara singkat dapat dinyatakan sebagai suatu ilmu sekaligus seni yang mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik. Jadi, yang dimaksud dengan peraturan hukum positif (the positive rules) dalam definisi Marc Ancel itu jelas adalah peraturan perundang-undangan hukum pidana. Dapat disimpulkan bahwa istilah penal policy menurut Marc Ancel adalah sama dengan istilah kebijakan atau politik hukum pidana.

2.3.1. Kebijakan Penal

Sarana ”penal” merupakan ”penal policy” atau ”penal law enforcement policy” sangat vital perannya dalam proses penegakan hukum untuk menanggulangi kejahatan. Seminar kriminologi ke-3 tahun 1976 dalam salah satu kesimpulannya menyebutkan: Hukum pidana hendaknya dipertahankan sebagai salah satu sarana untuk *sosial defence* dalam arti melindungi masyarakat terhadap kejahatan dengan memperbaiki atau memulihkan kembali (rehabilitatie) si-pembuat tanpa mengurangi keseimbangan kepentingan perorangan (pembuat) dan masyarakat.[44]

---

[43] Aloysius Wisnusubroto. 1999. *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Yogyakarta : Universitas Atmajaya, halaman 3

[44] Muladi dan Barda Nawawi Arief. 1998. *Teori-Teori dan Kebijakan Pidana*, Bandung : Alumni, halaman 92

Politik kriminal yang dilakukan dengan menggunakan sarana penal berarti penggunaan sistem peradilan pidana, mulai dari kriminalisasi sampai dengan pelaksanaan pidana. Pendekatan dengan sarana penal harus terus menerus dilakukan melalui pelbagai usaha untuk menyempurnakan sistem peradilan pidana, baik dari aspek legislasi (kriminalisasi, dekriminalisasi dan depenalisasi), perbaikan sarana-prasarana sistem, peningkatan kualitas sumber daya manusia, dan peningkatan partisipasi masyarakat dalam sistem peradilan pidana. Secara sistemik, sistem peradilan pidana ini mencakup suatu jaringan sistem peradilan (dengan sub sistem kepolisian, kejaksaan, pengadilan dan pemasyarakatan) yang mendayagunakan hukum pidana sebagai sarana utamanya. Hukum pidana dalam hal ini mencakup hukum pidana materiil, formil dan hukum pelaksanaan pidana.[45]

Operasionalisasi kebijakan hukum dengan sarana ”penal” (pidana) dapat dilakukan melalui proses yang terdiri atas tiga tahap yakni:[46]

a. Tahap formulasi (kebijakan legislatif)
b. Tahap aplikasi (kebijakan yudikatif/yudisial)
c. Tahap eksekusi (kebijakan eksekutif/administratif).

2.3.2. Kebijakan Non Penal

Penerapan kebijakan non penal lebih menitiktekankan terhadap tindakan pencegahan sebelum terjadinya kejahatan. Pencegahan kejahatan (upaya non penal) memfokuskan diri pada campur tangan sosial, ekonomi dan pelbagai area

---

[45] Muladi, *Demokratisasi Hak Asasi Manusia dan Reformasi Hukum di Indonesia.* 2002. Jakarta : The Habibie Center, halaman 156 dan 182.

[46] Barda Nawawi Arief. 2007. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta : Kencana Prenada Media Group, halaman 78-79

kebijakan publik dengan maksud mencegah terjadinya kejahatan. Bentuk lain dari keterlibatan masyarakat, nampak dari upaya pencegahan situasional dan peningkatan kapasitas masyarakat dalam penggunaan sarana kontrol sosial informal. Peningkatan pencegahan kejahatannya berorientasi pada pelaku atau *offender-centred crime prevention* dan berorientasi pada korban atau *victim-centred crime prevention*.[47]

Tujuan utama dari usaha-usaha non penal bagaimana mampu memperbaiki kondisi-kondisi sosial tertentu, secara langsung mempunyai pengaruh preventif terhadap kejahatan. Upaya keseluruhan kegiatan preventif non penal itu memiliki kedudukan strategis dalam memegang posisi kunci yang seyogianya terus diintensifkan dan diefektifkan.

2.4. Pemanfaatan Kemajuan Teknologi sebagai upaya Pencegahan *Cyberbullying* melalui *Techno Prevention*

Dalam konteks *cyber crime* ini erat hubungannya dengan teknologi, khususnya teknologi komputer dan telekomunikasi sehingga pencegahan *cyber crime* dapat digunakan melalui saluran teknologi atau disebut juga techno-prevention. Langkah ini sesuai dengan apa yang telah diungkapkan oleh International Information Industri Congress (IIIC) sebagai berikut :[48]

> *The IIIC recognizes that government action and internasional treaties to harmonize laws and coordinate legal procedures are keying the fight cyber crime, but warns that these should not be relied upon as the only instrument. Cyber crime is enabled by technology and requires as healty reliance on technology for its solution.*

---

[47] Abintoro Prakoso, 2013. *"Kriminologi Hukum & Hukum Pidana"*, Yogyakarta : Penerbit Laksbang Grafika, halaman 159

[48] Barda Nawawi Arief. 1998. *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, Bandung: PT Citra Aditya Bakti, halaman 5

Pendekatan teknologi ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau cultural ini perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah cyber crime dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan. Pentingnya pendekatan budaya ini, khususnya upaya mengembangkan kode etik dan perilaku (code of behavior and ethics) terungkap juga dalam pernyataan IIIC sebagai berikut:[49]

> *IIIC members are also committed to participate in the development of code behaviour and ethics around computer and Internet use, and in campaigns for the need for ethical and responsible online behaviour. Given the international reach of Internet crime, computer and Internet users around the world must be made aware of the need for high standards of conduct in cyber space.*

Dalam jurnal James M. Byrne (Hukum Pidana dan Kriminologi, Universitas Massachusetts, Lowell) dan Gary T. Marx (Profesor Emeritus di MIT (Massachusetts Institute of Technology)) dalam jurnalnya yang berjudul "Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact", ada 2 (dua) bentuk inovasi dalam teknologi yang dapat diterapkan sebagai upaya pencegahan kejahatan di bidang teknologi : yaitu *Hard Technology* dan *Soft Technology*. Inovasi *Hard Technology* terdiri atas perangkat keras yang digunakan sebagai upaya mencegah kejahatan. Seperti adanya CCTV , detektor logam di sekolah-sekolah, bagasi skrining di

[49] *Ibid*

bandara, peluru bukti windows teller di bank, dan sistem keamanan di rumah dan bisnis. [50]

Soft Technology melibatkan penggunaan strategis informasi untuk mencegah kejahatan (mis yang pengembangan penilaian risiko, dan ancaman instrumen penilaian) dan untuk meningkatkan kinerja polisi (misalnya teknologi prediksi kepolisian, dan merekam / kemampuan streaming di kendaraan polisi). Inovasi *Soft Technology* termasuk program perangkat lunak baru, sistem klasifikasi, teknik analisis kejahatan, dan berbagi data / sistem teknik integrasi. [51]

[50] *Innovations in criminal justice technology can be divided into two broad categories: hard technology (hardware or materials) and soft technology (computer software, information systems). Hard technology innovations include new materials, devices, and equipment that can be used to either commit crime or prevent and control crime. An initial distinction can be made between criminal justice innovations that have a hard material base as against a less tangible information soft base (even if in practice these are often interwoven).We increasingly see hard technologies intended to prevent crime – the ubiquitous CCTV cameras, metal detectors in schools, baggage screening at airports,bullet proof teller windows at banks, and security systems at homes and businesses.*

[51] *Soft technologies involve the strategic use of information to prevent crime (e.g. the development of risk assessment, and threat assessment instruments) and to improve the performance of the police (e.g. predictive policing technology, and recording/video streaming capabilities in police vehicles). Soft technology innovations include new software programs, classification systems, crime analysis techniques, and data sharing/system integration techniques.*

BAB 3

KERANGKA KONSEPTUAL

Dalam hal ini penyusunan tesis sebagai penelitian hukum adalah terhadap masalah bagaimana hukum pidana dapat mengkrimininalisasi kejahatan *cyberbullying.* Karena Undang-Undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik tidak mengatur dengan jelas mengenai permasalahan kejahatan *cyberbullying* di Indonesia.

Kejahatan *cyberbullying* di Indonesia sangat erat kaitannya dengan kegiatan sehari-hari yang menuntut kita harus memanfaatkan teknologi setiap saat. Kejahatan *cyberbullying* sangat sulit dibuktikan apabila pelakunya menggunakan akun palsu. Sehingga hal ini memungkinkan semakin banyaknya kejahatan *cyberbullying* yang bahkan bisa mengakibatkan hilangnya nyawa seseorang. Adanya peraturan yang terdapat dalam KUHP dan UU ITE ternyata tidak membuat jera pelaku *cyberbullying*. Dalam menanggulangi kejahatan tersebut, dibutuhkan upaya secara penal dan non penal. Namun apabila upaya penal saja saat ini tidak cukup untuk menanggulangi kejahatan tersebut, maka dibutuhkan kebijakan integral hukum pidana dengan mengintegralkan upaya penal dan upaya non penal. Adapun upaya non penal tersebut adalah pendekatan di bidang teknologi (*Techno Prevention*).

Upaya pencegahan kejahatan *cyberbullying* menggunakan *Techno Prevention* tersebut adalah salah satu bentuk penanggulangan dengan menggunakan teknologi, dimulai dengan menciptakan keamanan dalam sistem

elektronik informasi dan komunikasi yang digunakan. Baik komputer, laptop , teleponseluler dan perangkat elektronik lainnya.

Beberapa teori yang dipergunakan sebagai pisau analisis dalam membahas rumusan masalah dalam kaitannya dengan *cyberbullying* :

1) Teori Kebijakan Hukum Pidana

Kamus besar Bahasa Indonesia memberikan arti terhadap istilah "politik" dalam 3 (tiga) batasan pengertian yaitu : 1) pengetahuan mengenai ketatanegaraan (seperti sistem pemerintahan, dasar-dasar pemerintahan), 2) segala urusan dan tindakan (kebijakan, siasat dan sebagainya), 3) cara bertidak (dalam menghadapi atau menangani suatu masalah) kebijakan.[52]

Dengan demikian kebijakan pidana *(penal policy/criminal law policy/strafrechtspolitiek)* dapat didefinisikan sebagai "usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang. Kata "sesuai" dalam pengertian tersebut mengandung makna "baik" dalam arti memenuhi syarat keadilan dan dayaguna.[53]

Dalam hal ini A.Mulder mengemukakan bahwa kebijakan hukum pidana ialah garis kebijakan untuk menentukan:[54]

i. seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu dirubah atau diperbaharui;
ii. apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana;
iii. cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan

[52] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* Op.Cit. halaman 27

[53] Aloysius Wisnubroto,*Op. Cit,* halaman 10

[54] *Ibid,* halaman 12

2) Teori Kriminalisasi

Sudarto berpendapat, pengertian kriminalisasi adalah proses penetapan suatu perbuatan orang sebagai suatu tindak pidana. Proses tersebut diakhiri dengan terbentuknya undang-undang yang mengatur bahwa perbuatan tersebut merupakan tindak pidana yang diancam pidana.[55] Teori Kebijakan Kriminalisasi adalah proses penetapan suatu perbuatan orang sebagai perbuatan yang dapat dipidana. Proses ini diakhiri dengan terbentuknya undang-undang dimana perbuatan itu diancam dengan suatu sanksi berupa pidana. Barda Nawawi Arief mengatakan bahwa sebagai suatu kebijakan kriminalisasi dapat diartikan sebagai suatu proses untuk menentukan perbuatan apa yang akan dilarang karena membahayakan atau merugikan, dan sanksi apa yang akan dijatuhkan, maka sistem peradilan pidana dapat diartikan sebagai proses penegakan.[56] Kriminalisasi adalah suatu perbuatan atau suatu hal menjadi suatu tindakan yang sebelumnya bukan merupakan suatu perbuatan yang dapat dipidana menjadi perbuatan yang dapat dipidana.

Dalam konteks ini, yang dimaksud kriminalisasi *cybercrime* sebenarnya kriminalisasi perbuatan-perbuatan yang dilakukan dalam dunia *cyber (Cyberspace)*, karena istilah kriminalisasi *cybercrime* sudah bermakna kejahatan di bidang maya/ virtual (*cyber*), sehingga digunakan istilah

[55] Sudarto, *Kapita Selekta Hukum Pidana,* Almuni, Bandung, 1981, halaman 31-32

[56] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Penanggulangan Kejahatan*, Citra Aditya Bhakti, Bandung, 2001, hlm.74

kriminalisasi *cybercrime* berarti mengkriminalkan kejahatan bukan mengkriminalkan perbuatan.[57]

3) Teori Kebijakan Intergral

Usaha penanggulangan kejahatan lewat pembuatan undang-undang (hukum) pidana pada hakikatnya merupakan bagian integral dari usaha perlindungan masyarakat *(sosial defence)* dan usaha mencapai kesejahteraan masyarakat *(sosial welfare)*. Kebijakan atau politik hukum pidana juga merupakan bagian integral dari kebijakan atau politik sosial (sosial policy*)*. Kebijakan sosial *(sosial policy)* dapat diartikan sebagai segala usaha yang rasional untuk mencapai kesejahteraan masyarakat dan sekaligus mencakup perlindungan masyarakat. Jadi, di dalam pengertian *"sosial policy*" sekaligus tercakup di dalamnya *"sosial welfare policy"* dan *"sosial defence policy*". Dilihat dalam arti luas, kebijakan hukum pidana dapat mencakup ruang lingkup kebijakan di bidang hukum pidana material, dalam bidang hukum pidana formal dan bidang hukum pelaksanaan pidana.

Upaya penanggulangan kejahatan perlu ditempuh dengan kebijakan, dalam arti : ada keterpaduan *(integralitas)* antara politik kriminal dan politik sosial; ada keterpaduan *(integralitas)* antara upaya penanggulangan kejahatan dengan "*penal" dan "non-penal".*

Penegasan adanya upaya penanggulangan kejahatan diintegrasikan dengan keseluruhan kebijakan sosial dan perencanaan pembangunan. Bahwa apabila hukum pidana hendak dilibatkan dalam usaha mengatasi segi-segi

[57] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara,* Op. Cit. Halaman 57

negatif dari perkembangan masyarakat/ modernisasi (antara lain penanggulangan kejahatan), maka hendaknya dilihat dalam hubungan keseluruhan politik kriminal atau *sosial defence planning*, dan merupakan bagian integral dari rencana pembangunan nasional.

Mengingat sebab-sebab terjadinya *cyberbullying* sangat kompleks, sehingga tidak dapat jika hanya diatasi dengan hukum pidana, karena hukum pidana merupakan bagian kecil (sub-sistem) dari sarana kontrol sosial. Di samping itu, sistem pemidanaan hanya bersifat fragmentair dan individual atau personal dan tidak bersifat struktural atau fungsional. Itu sebabnya, untuk lebih berfungsinya hukum pidana memerlukan sarana pendukung yang lebih bervariasi.[58]

Upaya pencegahan kejahatan yang integral mengandung arti, bahwa masyarakat dengan seluruh potensinya harus dipandang sebagai bagian dari politik kriminal. Sehubungan dengan hal ini, Kongres PBB menekankan, bahwa *"the over all organization of society should be considered as anti criminogenic"* dan menegaskan bahwa *"community relations were the basis for crime perevention programs."* Perlu untuk membina dan meningkatkan efektivitas "extra-legal system" *atau "informal system"* yang ada di masyarakat dalam usaha penanggulangan kejahatan, antara lain kerjasama dengan organisasi sosial dan keagamaan, lembaga-lembaga pendidikan dan organisasi *volunteer* yang ada di masyarakat.

---

[58] Arief Amrullah, makalah *Membangun Komintemn bersama dalam Menegakkan Hukum tanpa Suap* (Perspektif Pendekatan Kebijakan Secara Integral, Seminar Nasional diselenggarakan oleh DPC PERADI Malang, dengan tema "Membangun Komitmen Bersama Dalam Menegakkan Hukum Tanpa Suap, tanggal 17 Desember 2016

Sistem peradilan (atau sistem penegakan hukum – untuk selanjutnya disingkat SPH) dilihat secara integral, merupakan satu kesatuan berbagai sub-sistem (kompo-nen) yang terdiri dari komponen ”substansi hukum” (*legal substance*), ”stuktur hukum” (*legal structure*), dan ”budaya hukum” (*legal culture*). Sebagai suatu sistem penegakan hukum, proses peradilan/penegakan hukum terkait erat dengan ketiga komponen itu, yaitu norma hukum/peraturan perundang-undangan **(**komponen substantif/ normatif**)**, lembaga/struktur/aparat penegak hukum (komponen struktu-ral/institusional beserta mekanisme prosedural/ administrasinya), dan nilai-nilai budaya hukum (komponen kultural**)**. Yang dimaksud dengan nilai-nilai “budaya hukum” (*legal culture)*dalam konteks penegakan hukum, tentunya lebih terfokus pada nilai-nilai filosofi hukum, nilai-nilai hukum yang hidup dalam masyarakat dan kesadaran/sikap perilaku hukum/perilaku sosialnya, dan pendidikan/ilmu hukum.[59]

Dilihat dari sudut politik kriminal, masalah strategis yang justru harus ditanggulangi ialah menangani masalah-masalah atau kondisi sosial secara langsung atau tidak langsung dapat menimbulkan kejahatan. Penanganan masalah-masalah merupakan posisi kunci dan strategis dari sudut politik kriminal.

---

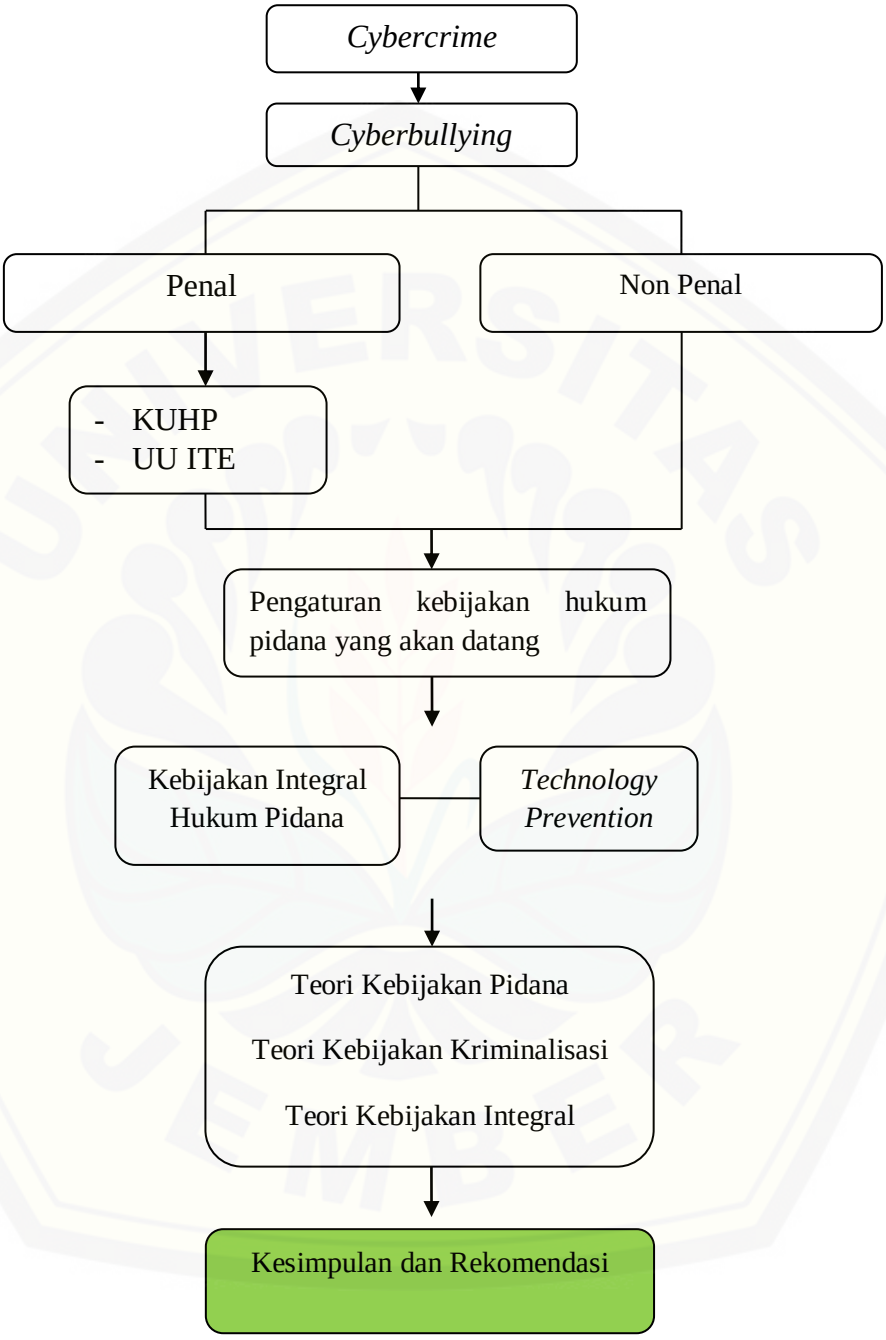
[59] L. Friedman, 1984. **“What Is a Legal System”** dalam **American Law.** W.W. Norton & Company, New York, hal. 2.menjelaskannya sbb. : *Other elements in the system are cultural. These are the values and attitudes wich bind the system together and wich determine the place of the legal system in the culture of the society as a whole; ..... the legal culture, that is, the network of values and the attitudes relating to law, wich determines when and why and where people turn to the law, or to government, or turn away.* Dalam Lawrence M. Friedman : **American Law in the 20th Century**, Yale University Press New Haven and London, 2002, h. 505 : ….. *the general legal culture: the attitudes, opinions, and points of view of the population as a whole—lay people, whether investment bankers, factory workers, nurses, bus drivers, or anybody else.*

Menyadari tentang pentingnya pengaturan mengenai *cyberbullying* sebagai salah bagian/jenis dari cyber crime yang memanfaatkan teknologi internet maka, pengaturan mengenai internetlah yang seharusnya dilakukan. Jika dilhat dari sudut metode pendekatan teknologi (*techno prevention*) ini, untuk menahan gencarnya penyalahgunaan pemakaian internet oleh para kaum *hacker* dan *cracker*.

Pendekatan teknologi (*techno-prevention*) yaitu upaya pencegahan/penanggulangan kejahatan dengan menggunakan tekhnologi. Perlunya penanggulangan kejahatan *cyber crime* secara teknologi diungkapkan oleh IIIC (*International Information Industry Congress*) yang mengakui bahwa tindakan pemerintah dan perjaanjian internasional untuk mengharmonisasikan hukum dan mengkordinasikan prosedur hukum merupakan kunci dalam upaya penanggulangan *cyber crime*, namun patut diingat bahwa hal ini janganlah diandalkan sebagai satu-satunya alat. *Cybercrime* dimungkinkan (terjadi) oleh tekhnologi dan (oleh karena itu) memerlukan suatu kepercayaan yang baik pada teknologi untuk pemecahannya.[60]

[60] Barda Nawawi Arief. 2002. *Sari Kuliah Perbandingan Hukum Pidana*, Jakarta : Raja Grafindo Persada, halaman 254-255.

Teori tersebut di atas dipergunakan untuk menganalisis permasalahan dalam tesis sebagaimana diuraikan dalam bagan berikut :



BAB 5

PENUTUP

1.1. Kesimpulan

Berdasarkan uraian pada bab-bab sebelumnya, dapat dikemukakan beberapa kesimpulan sebagai berikut :

1. Pencegahan kejahatan *cyberbullying* secara menyeluruh belum dapat dicapai dengan sarana hukum pidana saat ini. Meskipun telah ada UU ITE, namun dalam pelaksanaannya banyak kendala yang dihadapi oleh penegak hukum. Hal ini karena terdapat beberapa keterbatasan hukum pidana untuk mencegah kejahatan *cyberbullying*. Berkenaan dengan beberapa keterbatasan tersebut, kebijakan penerapan hukum pidana perlu diimbangi dengan kebijakan nonpenal. Bahkan kebijakan non penal mempunyai peranan yang sangat strategis dalam penanggulangan kejahatan *cyberbullying.*
2. Formulasi pencegahan *cyberbullying* didasarkan pada upaya menghilangkan sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan tersebut. Dalam mengsinergikan kebijakan penal dan non penal perlu adanya pendekatan yang berorientasi pada kebijakan (*policy oriented approach*). Permasalahan utama dalam mengintregasikan dan mengharmonisasikan kebijakan penal dengan nonpenal kearah penekanan dan pengurangan faktor-faktor potensial yang menumbuhsuburkan kejahatan. Melalui pendekatan intergral tersebut diharapkan pelaksanaan rencana perlindungan masyarakat (*social defence planning*) berhasil. Keberhasilan tersebut dapat menopang pencapaian tujuan kebijakan sosial yang tertuang dalam rencana pembangunan nasional.

1.2. Saran

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

1. Hukum pidana masih mempunyai keterbatasan untuk menanggulangi kejahatan *cyberbullying*, maka dari itu penanggulangan tidak hanya dilakukan dengan mengaplikasikan Undang-undang saja. Seharusnya, upaya pencegahan non penal dengan menitikberatkan pada edukasi kepada masyarakat tentang kode etik menggunakan jejaring sosial. Selain itu, seharusnya pencegahan di bidang teknologi juga dengan meningkatkan kemanan sistem informasi.
2. Seharusnya perlu segera dibahas dan dibuat peraturan mengenai Tindak Pidana di bidang Teknologi Infomasi karena RUU ini dapat menjadi pelengkap UU ITE untuk lebih meningkatkan kemampuan hukum pidana dalam pemberantasan kejahatan *cyberbullying* di Indonesia.

DAFTAR BACAAN

A. Buku Literatur

Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara* (*Cyber Crime*), Jakarta: PT. Refika Aditama

Abintoro Prakoso, 2013, *"Kriminologi Hukum & Hukum Pidana"*, (Penerbit Laksbang Grafika -Yogyakarta)

Agus Rahardjo, 2002, *Cybercrime-Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti.

Aloysius Wisnubroto, 1999, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer,* Yogyakarta, Universitas Atmajaya

Arief Amrullah, makalah *Membangun Komintmen bersama dalam Menegakkan Hukum tanpa Suap* (Perspektif Pendekatan Kebijakan Secara Integral, Seminar Nasional diselenggarakan oleh DPC PERADI Malang, dengan tema "Membangun Komitmen Bersama Dalam Menegakkan Hukum Tanpa Suap, tanggal 17 Desember 2016

Barda Nawawi Arief, 1982, *Masalah Pemidanaan Sehubungan dengan Perkembangan Delik-delik Khusus Dalam Masyarakat Modern*, Bandung: Banacipta, (Selanjutnya di sebut dengan Barda Nawawi Arief II)

_____,1984, *Pelengkap Bahan Kuliah Hukum Pidana I*, Semarang: FH-UNDIP

_____, 1988, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, Bandung: PT. Citra Aditya Bakti

_____,2002, *Bunga Rampai Hukum Pidana*,Bandung : PT. Citra Aditya Bakti

_____,2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidanadalam Penanggulangan Kejahatan*, Jakarta: Kencana Predana Media Group.

_____,2005, *Tindak Pidana Mayantara*, Jakarta : Raja Grafindo Persada

Bambang Poernomo, 1988, *Kapita Selekta Hukum Pidana*, Yogyakarta : Liberty

Didik J.Rachbini, 2001, *"Mitos dan Implikasi Globalisasi"* : Catatan Untuk Bidang Ekonomi dan Keuangan, Pengantar edisi Indonesia dalam Hirst, Paul dan Grahame Thompson, Globalisasi adalah Mitos, Jakarta, YayasanObor.

Dikdik M. Arief Mansyur dan ElisatrisGultom, 2005, *Cyber Law aspek Hukum Teknologi Informasi* (Refika Aditama; Bandung)

Deris Setiawan, 2005, *Sistem Keamanan Komputer*, Jakarta : PT Elex Media Komputindo

Dewi Astutty Mochtar,dkk. 2012, *Pengantar Ilmu Hukum*. (Malang: Bayumedia Publishing

G. Peter Hoefnagels, 1969, *The Others Side of Criminology*, Holland : Kluet-Devender

Henry Campbell Black,"Black's Law Dictionary", Seventh Edition, 1999 St.PaulminWest Publicing,Co.

J.J.H Bruggink, 1996, Alih Bahasa Arief Sidharta, *Refleksi tentang Hukum*, Bandung, Citra AdityaBakti

Johnny Ibrahim, 2008 ,*Teori dan Metodologi Penelitian Hukum Normatif*. Malang:Banyumedia Publishing, 2008

Kartika Risna, 2014,*Pencegahan Perilaku Bullying di Lingkungan*, Serambi, Jakarta

Kathryn Gerald, 2012 ,*Intervensi Praktis Bagi Remaja Beresiko* (Yogyakarta: Pustaka Pelajar

Muladi, 2002, *Demokrasi, Hak Asasi Manusia dan Reformasi Hukum di Indonesia*, Jakarta, Habibie Center

Muladi dan Barda Nawawi Arief, 1998, *Teori-Teori dan Kebijakan Pidana*, Bandung: Alumni

_____, 1998, *Kapita Selekta Hulum Pidana,* Bandung : Alumni

Peter Mahmud Marzuki. 2014, *Penelitian Hukum*, Jakarta : Kencana Prenada Media Group

Roeslan Saleh, 1982, *Pikiran – Pikiran tentang Pertanggungjawaban Pidana*, Jakarta: Ghalia Indonesia

Romli Atmasasmita, 1989, *Asas – Asas Perbandingan Hukum Pidana*, Jakarta: Yayasan Lembaga Bantuan Hukum Indonesia

Sheri Bauman, Donna Cross and Jenny Walker, 2013, *Principles of Cyberbullying* (New York: Taylor ang Francis Group),

Sudarto, 1990, *Hukum Pidana I*, Semarang : Yayasan Sudarso

Soedarto, 1981, *Hukum dan Hukum Pidana*, Bandung: Alumni

_____,1981, *Kapitas Selekta Hukum Pidana*, Bandung : Alumni

Summary Report, 1974, *Resource Material* No. 7, UNAFEI

Soerjono Soekant, 1982, *Kesadaran Hukum dan Kapetuhan Hukum*, Jakarta : Rajawali

Soerjono Soekanto dan Abdurrahman. 2003.*Metode Penelitian Hukum*. Jakarta:Rineka Cipta

Widodo, 2011, *Aspek Hukum Pidana Kejahatan Mayantara,* Yogyakarta : Aswaja Pressindo

B. Peraturan Perundangan

Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Kitab Undang-Undang Hukum Pidana;

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana;

Undang-Undang Nomor 19 tahun 2016 Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

C. Sumber Internet

http://www.beritasatu.com/dunia/77339-tak-tahan-di-bully-seorang-remaja-putri-bunuh-diri.html diakses

http://www.jpnn.com/read/2013/05/28/174068/Sempat-Pesan-Ingin-Dimakamkan-di-Dekat-sang-Kakek

Ari Juliano Gema, 2000, *Cyber Crime : Sebuah Fenomena di Dunia Maya".* www.thecelli.com

http://mycyberbullying.wordpress.com/2014/05/25/pengertian-cyberbullying/,diakses padaSabtu, 27 Januari 2017, pukul 19:40 WIB

International Review of Criminal Policy-United Nations Manual on The Prevention And Control of Computer-Related Crime,http://www.uncjin.org

"Cybercrime Indonesia Tertinggi di Dunia", www.polri,go.id diakses 29 Maret 2017

Michael A. Vatis, 2000, *"Statement of Record on Cybercrime",* http://www.fbi.gov/pressrm/congresso2htm, diakses tanggal 30 Maret 2017

Mukhlis Ifransah, *"Perlindungan Hukum HKI di Era Digital".* www.hukumonline.com diakses 12 Juni 2017

www.ncpc.org/resources/cyberbullying , *Stop Cyberbullying Before ot Starts",* diakses 17 April 2017

https://www.stopbullying.gov/cyberbullying/prevention diakses 17 Juni 2017

http://www.internetsafety/ pada tanggal 24 Maret 2017

http://www.thecybersafety.com/ diakses 24 Maret 2017

http://www.addictinggames,com/ diakses 27 Maret 2017

http://www.smallworlds.com/ diakses pada tanggal 27 Maret 2017

http://www.androidauthority.com/ diakses tanggal 27 Maret 2017

D. Lain-lain

Doni Budi Utomo, *Komunitas Internet Indonesia Terkenal Embargo,* Kompas, tanggal 29 November 2012

Firhot Patra Sinaga, 2005, *Analisis Kebijakan Kriminal terhadap Penanggulangan Kejahatan Teknologi Informasi,* Skripsi, Fakultas Hukum Universitas Lampung

Hogan Kusnandi, "*Praktik Kejahatan dalam Bidang Telematika"* , Makalah dalam Seminar Nasional tentang Strategi Penanggulangan Kejahatan dalam Bidang Telematika. Hotel Patra Jasa Semarang, 23 Juli 2002

Sutrisman, *"Penanggulangan Kejahatan Bidang Telematika dalam Perspektif Operator Telekomunikasi",* Makalah dalam Seminar Nasional tentang Strategi Penanggulangan Kejahatan dalam Bidang Telematika. Hotel Patra Jasa Semarang, 23 Juli 2002

"Indonesia bentuk ID-First", Harian Sinar Harapan edisi 21 Maret 2003

Tribun Jabar, 9 Desember 2015 *Amerika dan China Tingkatkan Kerjasama Cybercrime*

www.kompas.com 19 Desember 2015, Fabian Januarius Kuwado, *Polisi Cyber Crime RI Cuma 18 personel, Polisi China geleng-geleng kepala*