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

Oleh :

Firda Laily Mufid
Email : firdalaily25@gmail.com

Abstract

Cybercrime is human activity in the world mayantara who has made the computer as the evil deeds for example illegal access, to the destruction of the site , the interception of illegal , and the activities of humans which uses computers as the evil of the target credit card forgery for example, pornography via the internet. One of evil in the world mayantara namely cyberbullying that is a form of intimidation the guilty person or more to pigeonhole, discredit, to men through cyberspace. This intimidation do not haphazardly as a result, it was not uncommon death be the end of cyberbullying. Cyberbullying too are defined as a form of intimidation to which the offender do to harass his victims through technology device. Investors want to see someone gets hurt , there are a lot of the way they do to strike the victim with a message cruel and pictures of a disturbing and disseminated in order to embarrass incense to anyone

Keywords: *Cybercrime, cyberbullying, intimidation, technology*

PENDAHULUAN

A. Latar Belakang

Pengguna *internet* di Indonesia dari tahun ke tahun semakin meningkat. Data yang diperoleh dari *Internet World Statistics* menunjukkan jumlah pengguna 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.[1]

Pemanfaatan teknologi *internet* juga tidak dapat dipungkiri membawa dampak negatif yang tidak kalah banyak dengan manfaat positif yang ada. *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.[2]

Berdasarkan data dari *Clear Commerce* tahun 2002 Indonesia di-posisikan 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.[3]

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

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

[2] 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.

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

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).[4]

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.*

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.

[4] *Ibid*

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.[5]

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 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.

Dalam perspektif lain, dalam pasal 3 UU ITE, teknologi informasi menjadi mungkin dalam formatnya saat inikarena 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

[5]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

lain sebagainya. Adapun *software* antara lain terdiri dari kelompok: sistem operasi, *data base*, sistem aplikasi, dan bahasa pemrogaman (*progamming language*).

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.

B. Perumusan Masalah

Bertumpu pada latar belakang diatas, permasalahan penelitian dapat dirumuskan permasalahan tentang bagaimana formulasi kebijakan integral hukum pidana dengan menggunakan sarana *Techno Prevention* sebagai upaya pencegahan kejahatan *cyberbullying* di masa yang akan datang?

PEMBAHASAN

A. Kebijakan Integral Hukum Pidana dengan *Techno Prevention* sebagai Upaya Pencegahan Kejahatan *Cyberbullying*

Kebijakan atau upaya penanggulangan kejahatan pada hakikatnya merupakan bagian integral dari upaya perlindungan masyarakat *(social defence)* dan upaya mencapai kesejahteraan masyarakat *(social welfare)*, oleh karena itu dapat dikatakan bahwa tujuan akhir atau tujuan utama dari politik kriminal ialah "perlindungan masyarakat untuk mencapai kesejahteraan."

Istilah "kebijakan hukum pidana" dapat disebut dengan istilah "politik hukum pidana." Dalam kepustakaan asing istilah "politik hukum pidana" sering dikenal dengan berbagai istilah, *"Penal Policy", "Criminal Law Policy",* atau *"Strafrechtspolitiek."*

Pengertian kebijakan atau politik hukum pidana dapat dilihat dari politik hukum maupun dari politik kriminal, menurut Prof. Soedarto, "politik hukum" adalah usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi tertentu. Kebijakan dari Negara melalui Badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dapat digunakan

untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan.[6]

Penanggulangan kejahatan lewat jalur *"Penal"* lebih menitikberatkan pada sifat *"Repressive"* (Penindasan/ Pemberantasan/Penumpasan) sesudah kejahatan terjadi, sedangkan jalur "non-penal" lebih menitikberatkan pada sifat *"preventive*" (Pencegahan/ Penangkalan) sebelum kejahatan terjadi. Dikatakan sebagai perbedaan secara kasar, karena tindakan represif pada hakikatnya dapat dilihat sebagai tindakan preventif dalam arti luas.[7]

Kedudukan strategis *non penal* dalam upaya penanggulangan kejahatan dapat juga dilihat dalam Resolusi Kongres PBB VII/1990 mengenai "*Computer relate crimes*" yang mengajukan beberapa kebijakan dalam rangka upaya menanggulangi *cyber crime* antara lain sebagai berikut :[8]

a. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut :
   1. Melakukan modernisasi hukum pidana materiil dan hukum acara pidana;
   2. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
   3. Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan, dan penegak hukum terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer;
   4. Melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat, dan aparatur penegak hukum mengenai kejahatan ekonomi dan *cyber crime*;
   5. Memperluas "*rules of ethics*" dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika;
   6. mengadopsi kebijakan perlindungan korban *cyber crime* sesuai Deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime*;
b. mengimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cyber crime*;
c. merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*Committee on Crime Prevention and Control*) PBB untuk :

[6] Soedarto, 1981, *Hukum dan Hukum Pidana*, Bandung : Alumni, halaman. 159

[7] Soedarto, 1981, *Kapita Selekta Hukum Pidana*,Bandung :Alumni. halaman. 188

[8] Barda Nawawi Arief, 2008, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Prenada Media Group, halaman 238-239.

1. menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi *cyber crime* di tingkat nasional, regional dan internasional;
2. mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem *cyber crime* di masa yang akan datang;
3. mempertimbangkan *cyber crime* sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan

d. Resolusi Kongres PBB VII/1990 mengenai *Computer related crime* dalam upaya menanggulangi *cyber crime* di atas pada beberapa poin menegaskan bahwa dalam menanggulangi *cyber crime* lebih mengedepankan upaya *non penal* dengan cara melakukan penanggulangan. Resolusi Kongres PBB VII/1990 diatas berlaku juga untuk menanggulangi tindakan *cyber bullying*, karena *cyber bullying* merupakan salah satu bentuk dari *cyber crime* yang terjadi karena perkembangan teknologi yang pesat dan tidak diikuti dengan kesadaran penggunaan teknologi yang baik.

Melalui kebijakan nonpenal, Muladi menyatakan bahwa perlu juga dilakukan upaya berikut :

1) Kerjasama Internasional

Sifat *cybercrime* adalah transnsional, karena itu diperlukan kerjasama internasional yang intensif baik dalam penegakan hukum pidana maupun dalam bidang teknologi berupa pembentukan jaringan informasi yang kuat, misalnya program "*24 hours point cantact"* untuk menghadapi kejahatan *cybercrime*. Pelatihan personil penegak hukum yang memadai, harmonisasi hukum dan penyebarluasan kesepakatan-kesepakatan internasional. Sebagai contoh dalam aktivitas tersebut adalah *spontaneus information,* yakni suatu komitmen untuk tanpa diminta segera menyebarluaskan informasi bilamana ditemukan hal-hal negatif yang dapat dijadikan bahan investigasi, pembuktian, proses peradilan tentang *cybercrime* bagi negara lain.

2) Rencana Aksi Nasional (*National Action Plan*)di Indonesia

Dalam ruang lingkup nasional perlu disusun suatu rencana aksi nasional (*national plan of action*) untuk menanggulangi *cybercrime* khususnya *cyberbullying*, karena viktimisasi kejahatan tersebut sangat luas dan sifatnya transnasional. Pemerintah dan beberapa komunitas teknologi informasi nsional perlu menggalang kerjasama guna menanggulangi kejahatan di dunia maya

(*cybercrime*).[9] Kegiatan yang sudah dilakukan tersebut misalnya melalui pendirian *Indonesia Forum on Inromation for Infocom Incident Respomse adn Security Team* (ID FIRST), yang diharapkan menciptkan sinergi antara pemerintah, kepolisian, dan industri teknologi informasi dalam mencegah dan memberantas kejahatan dunia maya melalui internet.[10]

Berkenaan dengan penanggulangan *cybercrime* khususnya *cyberbullying* dengan menggunakan kebijakan kriminal, Ari Julianto Gema menjelaskan beberapa langkah penting yang dapat dilakukan oeh setiap negara dalam penanggulangan *cybercrime*, yaitu sebagai berikut. .[11]

a) Melakukan pembaruan hukum pidana materiel dan formel, yang diselaraskan dengan konvensi internsional yang terkait dengan *cybercrime;*
b) Meningkatkan sistem pengamanan jaringan komputer nasional sesuai dengan standar internasional;
c) Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yanmg berhubungan dengan *cybercrime;*
d) Meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya mencegah terjadinya kejahatan;
e) Meningkatkan kerjasama antarnegara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaties*

Langkah-langkah menanggulangi *cybercrime* adalah sebagai berikut:

a. Pertama, bahwa peran kita dalam penanggulangan terhadap *cybercrime* merupakan hal yang sangat utama, yaitu dengan dua cara; (1) pem-cegahan serangan dunia maya sebelum terjadi atau pembatasan ruang lingkupnya, yaitu dengan cara penyebarluasan nasigat dan peringatan tentang ancaman tersebut sehingga pihak yang potensial menjadi korban kejahatan dapat melindungi dirinya sendiri; dan (2) memberi tanggapan terhadap serangan yang terjadi dengan menyelidiki dan megidentifiasi pelaku;
b. Kedua, dalam pengumpulan informasi sebagai bagian dari peringatan dan tanggapan kita terhadap serangan tersebut, kita perlu mengikuti per-syaratan hukum dan peraturan perundang-undangan.

[9] *Ibid*
[10] *Indonesia Bentuk ID-First"*, Harian Sinar Harapan, 21 Maret 2003, halaman 8
[11] Ari Juliano Gema, *Cybercrime Sebuah Fenomena di Dunia Maya,* Majalah Infokom, halaman 12

Kerjasama penanggulangan *cyber-crime* sudah dilakukan Indonesia dengan perusahaan-perusahaan yang membidangi teknologi informasi misalnya *Microsoft Indonesia* dalam rangka mengidentifikasi *software* hasil bajakan dari *Microsoft Corporation* yang digunakan di Indonesia. Mukhlis Ifransyah mengemukakan, *Microdoft* memiliki sistem tersendiri untuk melakukan *scanning* atas material (*content*) di internet yang melanggar hak cipta atas *software* produksinya. Jika ditemukan pelanggaran hak cipta, pihak Microsoft akan meminta pihak lain tempat *software* bajakan di *posting* untuk melakukan tindakan pemutusan atas *service* tersebut dan menghapus material tersebut dari *server*. Meskipun demikian, hasil kerjasama tersebut belum menunjukkan hasil optimal.[12]

Cyberbullying sebagai bagian dari tindak pidana *cybercrim*e atau perbuatan yang menyalahgunakan teknologi internet dengan cara menghina, memfitnah serta memeras di dalam dunia maya (*cyber space*) yang akibatnya dapat mengakibatkan anak-anak menjadi stres, melukai diri sendiri (*self injury*), melakukan tindak kriminal, dan melakukan komitmen untuk bunuh diri (*commit suicide*), untuk penanggulangannya pun harus diorientasikan pada pengaturan penggunaan teknologi internet itu sendiri dan menanamkan etika kepada setiap pengguna teknologi yang berkembang pesat terkait dengan teknologi informasi dan komunikasi.

Pencegahan tehadap kejahatan *cyberbullying* membutuhkan sinergi antara masyarakat yang partisipatif dengan aparat penegak hukum yang demokratis, transparan, bertanggung jawab dan berorientasi pada HAM, pada alirannya diharapkan dapat benar-benar mewujudkan masyarakat madani Indonesia yang berkeadilan sosial. Selain itu, perlu adanya edukasi terhadap masyarakat untuk bijak dalam menggunakan teknologi serta tidak mudah percaya terhadap berita-berita yang belum jelas sumbernya.

Menurut Barda Nawawi Arief upaya penanggulangan *cyber crime* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*), pendekatan budaya (*cultural*), pendekatan edukatif/moral/ *religious*, bahkan pendekatan global (kerjasama internasional) karena melampaui batas-batas Negara atau *transnational*/ *transborder*.[13] Terdapat beberapa upaya dalam penanggulangan tindakan *cyber bullying* yaitu sebagai berikut :

1. Pendekatan Budaya (Kultural)

Sosialisasi etika *internet* serta akibat negatif dari tindakan *cyber bullying*

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

[13]Barda Nawawi Arief, 2008, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op. Cit.* Halaman 238-239

menjadi upaya penanggulangan *non penal* dalam srategi *preventif*. Sosialisasi etika *internet* ini sangat diperlukan agar masyarakat tahu bahwa di dunia maya juga ada norma-norma yang harus dipatuhi. Sehingga dapat mencegah terjadinya tindakan *cyber bullying* yang berakibat terhadap anak.

2. Pendekatan Pendidikan Moral (Edukatif)

Cassare Beccaria menyatakan metode yang paling tepat untuk mencegah kejahatan adalah dengan menyempurnakan sistem pendidikan.[14] Pendekatan pendidikan moral dan agama merupakan pendekatan yang sangat dibutuhkan dalam penanggulangan tindakan *cyber bullying*. Pendekatan moral dan agama adalah pendekatan yang strategis karena dapat semaksimal mungkin mengurangi potensi untuk melakukan tindak intimidasi di duna maya, serta akan lebih dapat menumbuhkan kesadaran dari setiap orang untuk menghindari tindakan *cyber bullying* dengan media elektronik dengan jenis apapun. Pendidikan moral dan agama diharapkan menjadi upaya preventif yang strategis dalam menanggulangi tindakan *cyber bullying*. Orang tua yang memahami bentuk pengawasan terhadap anak akan menekan tindakan *cyber bullying* yang dilakukan anak terhadap anak-anak lainnya. Tindakan tersebut sangatlah penting mengingat banyaknya anak-anak usia dini seringkali melakukan penghinaan dan menyebarkan berita-berita yang tidak benar di dunia maya.

Pendidikan moral dan peranan keluarga juga didukung oleh Mahmud Mulyadi Pakar Hukum Pidana dalam upaya penanggulangan kejahatan yang dapat dilihat dalam bukunya berjudul *"Criminal Policy : Pendekatan Integral Penal Policy dan Non-Penal Policy dalam Penanggulangan Kejahatan Kekerasan"*, dijelaskan bahwa kehangatan sebuah keluarga akan melahirkan motivasi yang positif para anggotanya dalam menghadapi kehidupan. Sebaliknya, kondisi keluarga yang berantakan, menjadikan anggota-anggotanya (terutama anak-anak) cenderung melakukan perbuatan yang menyimpang sehingga dapat mengarah terjadinya kejahatan.[15]

3. Pendekatan Ilmiah

Kebijakan yang rasional dalam menanggulangi tindakan *cyber bullying* tidak terlepas dari pendekatan ilmiah. Hal tersebut sesuai dengan pernyataan Marc Acel bahwa di perlukan usaha yang rasional dalam menanggulangi kejahatan.

[14] Wahmuji, 2011, *Perihal Kejahatan dan Hukuman*, Yogyakarta: Genta Publishing, halaman 149

[15] Mahmud Mulyadi, 2008, *Criminal Policy : Pendekatan Integral Penal Policy dan Non-Penal Policy dalam Penanggulangan Kejahatan Kekerasan*, Medan: Pustaka Bangsa Press, halaman 15.

Usaha yang rasional dapat dalam bentuk pendekatan ilmiah dalam mengkaji suatu tindakan *cyber bullying*. Pendekatan ilmiah menuntut perguruan tinggi dan akademisi melakukan penelitian, sosialisasi dan seminar terhadap kejahatan yang menggunakan teknologi seperti *cyber bullying*, baik melalui *Basic Research* (penelitian dasar yang mempunyai alasan intelektual, dalam rangka pengembangan ilmu pengetahuan) ataupun *Applied Research* (penelitian terapan yang mempunyai alasan praktis, keinginan untuk mengetahui dan bertujuan agar dapat melakukan sesuatu yang lebih baik, efektif, efisien). Pendekatan ilmiah sangat penting untuk menanggulangi maraknya tindakan *cyber bullying* dan dampak negatifnya.

4. Pendekatan Teknologi (Techno Prevention)

Pelaku *cyber bullying* memanfaatkan sarana teknologi untuk melakukan tindakan intimidasi terhadap anak. Oleh karena itu penggunaan sarana *non penal* harus melibatkan pendekatan teknologi juga sebagai langkah strategis dalam pencegahan tindakan *cyber bullying*. Penanggulangan tindakan *cyber bullying* menggunakan teknologi dapat dilihat dari upaya pemerintah dan lembaga-lembaga terkait lainya dalam menciptakan dan mengembangkan teknologi yang memberikan keamanan dan akses cepat dalam menanggulangi tindakan *cyber bullying*.

Cyberbullying umumnya terjadi dalam dunia maya dan melalui beberapa media di *internet* sebagai perantaranya. Berikut beberapa media yang ada di *internet* yang sering digunakan dan dikunjungi oleh anak maupun remaja yang perlu diwaspadai untuk mencegah terjadinya tindakan *cyberbullying* :

a. Jejaring sosial

Kasus *cyber bullying* banyak di dominasi jejaring sosial, dan tidak sedikit kasus bunuh diri yang terjadi berawal dari perkenalan di jejaring sosial.[16] Kebanyakan pengguna *internet* dikalangan remaja menggunakan jejaring sosial seperti *facebook, twitter, instagram* dll.

b. *Web Video* (*Video Hosting Service*)

Web video adalah situs berbagi video yang disediakan untuk membagikan video baik itu dokumenter milik pribadi maupun orang lain. Situs ini banyak dikunjungi anak-anak maupun orang dewasa. Salah satu situs *web video* yang terkenal adalah *youtube*. Dalam *web video* seperti *youtube* tidak sedikit video di upload atau diunggah penggunanya adalah video dengan konten-konten memiliki unsur kata-kata menghina dan melecehkan. Video dengan konten kata-kata menghina akan memberikan dampak negatif kepada penontonnya, yang dimana kebanyakan dari mereka adalah anak-anak yang relatif sering meniru hal-

[16] Diakses dari http://www.internetsafety/ pada tanggal 24 Maret 2017, pukul 15.30 WIB

hal yang dilihat. Selain video yang merisikan konten kata-kata kasar, dalam *video web* sering kali para penonton memberikan komentar yang pada akhirnya berujung saling menghujat dengan kata-kata kasar.[17] Jika anak sering melihat kata-kata kasar maka hal tersebut akan membuat tindakan *cyber bullying* akan mudah terjadi.

c. Game Online

Game online difasilitasi tombol komunikasi membuka peluang terjadinya tindakan *cyberbullying*, jika pemain menggunakan kata-kata kasar dan melakukan intimidasi dengan pemain lain. Apalagi *game online* identik dengan group atau komunitas, sehingga kemungkinan terjadinya diskriminasi cukup besar.[18]

d. Aplikasi *Video Call*

Aplikasi *video call* digunakan untuk melakukan interaksi sosial di dunia maya dengan cara bertatap muka secara langsung dengan sebuah aplikasi video.[19] Aplikasi seperti ini dapat juga menimbulkan tindakan *cyberbullying* jika pengguna tidak waspada terhadap penggunaannya. Kebanyakan anak-anak menggunakan aplikasi seperti ini dan bertemu dengan orang dikenal maupunyang tidak dikenal.

Dalam upaya pencegahan kejahatan *Cyberbully*, peran pemerintah juga sangat penting, adapun peran pemerintah dalam upaya penanggulangan kejahatan *cyberbullying* yang akan datang adalah :

1. Membentuk lembaga untuk menanggulangi tindakan *cyberbullying*

Di Selandia Baru dalam peraturan perundang-undangan *Harmful Digital Communications Bill* dibuat sebuah lembaga yang disetujui (*Approved Agency*) yang mempunyai fungsi untuk menerima laporan bagi siapa saja yang mendapatkan intimidasi tindakan *cyber bullying*. Di Selandia Baru lembaga ini diberi nama ***netsafe***, jika seseorang merasa mendapatkan tindakan yang mengarah kepada *cyber bullying*. Baik sebagai korban, orang tua, maupun orang terdekat dapat melaporkannya secara *online* kepada ***netsafe***. Indonesia harus mempunyai lembaga seperti ini untuk melindungi anak-anak bangsa terhindar dari tindakan *cyber bullying* yang ada di dunia maya. Dengan adanya lembaga seperti ***netsafe*** yang ada di Selandia Baru maka siapa saja dapat melaporkan jika terjadinya tindakan *cyber bullying*. Setelah dilaporkan maka lembaga yang telah ditunjuk akan memperoses apakah perbuatan termasuk kedalam tindakan *cyber bullying*.

Dalam hal ini, pemerintah Indonesia dapat membentuk suatu lembaga yang

[17] Diakses dari http://www.thecybersafety.com/ pada tanggal 24 Maret 2017, pukul 15.35 WIB

[18] Diakses dari http://www.addictinggames.com/ pada tanggal 27 Maret 2017, pukul 15.40 WIB

[19] Diakses dari http://www.androidauthority.com/ pada tanggal 27 Maret 2017, pukul 16,00 WIB

berfungsi untuk menerima laporan tidak hanya yang menjadi korban *cyberbullying*, tapi beberapa kejahatan yang terjadi di dunia maya. Seperti halnya laporan tentang penipuan melalui dunia maya ataupun kejahatan laiinya yang dikategorikan dalam kejahatan dunia maya. Karena selama ini, masyarakat Indonesia masih kesulitan untuk melaporkan kejahatan-kejahatan yang terjadi di dunia maya dan dibiarkan begitu saja. Hal tersebut yang menyebabkan kejahatan di dunia maya juga semakin banyak.

2. Membuat situs-situs anti *cyber bullying* untuk edukasi

Pemerintah juga harus membuat situs-situs yang membahas tentang upaya menanggulangi *cyber bullying* dan mengajarkan kepada pengguna *internet*, yang terutama adalah anak bagaimana cara mereka melindungi diri mereka dari tindakan *cyber bullying*. Setelah itu anak juga harus mendapat informasi tentang segalah berhubungan dengan tindakan *cyber bullying*. Bagaimana dampak negatif dari tindakan *cyber bullying* maupun bagaimana tahapan yang harus diperoleh oleh anak untuk menghadapi situasi ketika mereka berhadapan dengan pelaku tindakan *cyber bullying*. Situs yang dibuat tersebut bukan hanya untuk anak saja, melainkan juga diperuntukan untuk orang tua agar bisa lebih memahami tentang tindakan *cyber bullying* dan bagaimana melindungi anak mereka.

3. Menyelenggarakan seminar *internet* sehat dan anti *cyber bullying*

Para pihak seperti orang tua, anak-anak, guru, dan eksekutif *internet* berkumpul bersama dalam dalam forum *Wired Safety Internasional Stop Cyber-bullying Conference*. Eksekutif dari *facebook, verizon, Myspace*, dan *Microsoft* berbicara bagaimana untuk melindungi diri mereka sendiri, reputasi pribadi, anak-anak dan bisnis *online* agar terhindar dari pelecehan *online* dan tindakan *cyber bullying* lainnya. Dalam konfrensi di bahas tentang *cyber bullying* yang dikaitkan dengan hukum, dengan mendiskusikan tentang hukum yang mengatur tentang *cyber bullying* , bagaimana membedakan antara kekasaran dan pelecehan kriminal, menjelaskan tentang tanggung jawab hukum orang tua, kebutuhan hukum apa yang untuk lebih lanjut dibutuhkan dalam menanggulangi *cyber bullying*, bagaimana menangani postingan gambar, teks ataupun video yang berhubungan dengan pelecehan, perbedaan antara kebebasan berbicara dengan kebencian

4. Mensosialisasikan kembali UU ITE dan penggunaan *internet* yang baik

Target utama tindakan *cyberbullying* adalah anak, yang dimana dalam rentan usia mereka seringkali mudah untuk dipengaruhi. Pelaku dari tindak *cyber-*

bullying kebanyakan juga adalah anak, walaupun tidak menutup kemungkinan bahwa orang dewasa juga dapat melakukan tindakan *cyberbullying* terhadap anak. Hal ini dapat dilakukan dengan menjadikan materi UU ITE sebagai bahan ajar di sekolah. Seperti menyebutkan beberapa kegiatan yang dapat dikategorikan sebagai *cybercrime* dan apabila dilakukan akan dikenai sanksi. Karena masih banyak beberapa orang yang belum paham jika apa yang dilakukan tersebut dapat merugikan orang lain dan termasuk dalam *cybercrime.*

B. Konsep *Techno Prevention* sebagai Upaya Pencegahan Kejahatan *Cyberbullying*

Dalam penanggulangan *cyber bullying* dan kejahatan lainnya yang berhubungan dengan teknologi banyak perangkat lunak (*software*) yang digunakan untuk memberikan perlindungan bagi anak ketika menggunakan *internet* dan ter-hubung di dalam dunia maya. Aplikasi parental*control* dan penapis dapat di-gunakan untuk membantu melindungi keamanan anak di *internet* dan dipasang di berbagai jenis *gadget* yang digunakan. Beberapa aplikasi *parental control* yang dapat di pasang di antaranya adalah *Qustodio*, *K9 Web Protection*, *Kakatu* dan *DNS Nawala*. *Software* seperti *Kakatu* dan *DNS Nawala* adalah teknologi buatan Indonesia yang handal melindungi anak, sehingga seringkali kemenkoinfo dan komunitas yang peduli terhadap *internet* sehat dan menciptakan dunia maya yang aman, menganjurkan agar orang tua menggunakan *software* diatas untuk memberikan perlindungan terhadap anak.[20]

Software yang telah dijelaskan diatas dapat digunakan untuk mengetahui aktifitas anak di dunia maya saat terhubung dengan *internet*, situs-situs apa yang mereka sering masuki, memberikan peringatan jika situs yang dikunjungi memiliki konten berbahaya, dan pengguna *software* sendiri dapat melaporkan jika mengalami tindakan seperti *cyber bullying* maupun tindakan lain yang dianggap membahayakan dirinya .

Selain *software* yang bersifat melindungi pengguna *internet* yang dijelaskan diatas, diperlukan juga sistem keamanan yang menggunakan teknologi untuk melindungi komputer dan jaringannya agar tetap aman. Jika jaringan komputer dapat di kuasai oleh orang lain, maka akan muncul kemungkinan di-ambilnya data-data yang bersifat pribadi dan penting. Sehingga hal ini akan memunculkan kemungkinan terjadinya tindakan *cyber bullying*. Data-data pribadi tersebut dapat di sebarkan ke dalam dunia

[20] Diakses dari Internetsehat/id pada tanggal 27 Mei 2017, pukul 5:02 WIB

maya oleh orang yang tidak bertanggung jawab.

Berikut adalah empat aplikasi dan/ atau program perangkat lunak yang dirancang untuk membantu memerangi penindasan maya: [21]

(1) *Trend Micro Online Guardian*: *Trend Micro Online Guardian* didirikan oleh seorang ibu yang menyaksikan putrinya mengalami *cyberbullying* dan mengambil langkah besar untuk memperbaiki masalah. Online Guardian berisi kontrol komputer yang luas untuk melacak situs jejaring sosial populer seperti *Twitter, Facebook dan YouTube*. Perangkat lunak ini juga menawarkan manajemen pesan instan dan per-lindungan *malware*.

(2) *YouDiligence*: Orangtua tidak dapat selalu berada di sana secara langsung untuk menghentikan penindasan yang terjadi di dunia maya, tapi itu tidak berarti mereka tidak dapat melacak kejadian tersebut untuk membantu mencegah kejadian di masa depan. *YouDiligence* memungkinkan orang tua untuk memantau halaman jejaring sosial anak mereka sementara secara khusus melacak kata kunci yang terkait dengan intimidasi, ejekan rasial, alkohol, kata-kata kotor dan banyak lagi. Dengan daftar lebih dari 500 kata dan frase peringatan yang dapat diedit oleh orang tua berdasarkan spesifikasinya, *You Diligence* dapat mengirimkan lansiran email kepada orang tua bila ada aktivitas yang meragukan. Pembaruan ini kemudian dapat dikirim melalui email ke orang tua dan dilihat melalui dasbor online agar mudah dilacak.

(3) Perlindungan Jaringan Sosial Avira: *Avira Social Network Protection* adalah program perangkat lunak lain yang diciptakan sebagai hasil dari orang tua yang menyaksikan anak mereka mengalami *cyberbullying*. *Avira Social Network Protection*, yang sebelumnya dikenal dengan Social Shield, membedakan dirinya dari program anti-*cyberbullying* lainnya dengan memantau situs jejaring sosial agar tidak hanya melindungi dari intimidasi, namun juga menjaga reputasi anak. Perangkat lunak ini menggunakan perangkat lunak ber-basis awan, sehingga dapat diakses hampir di manapun melalui komputer atau telepon. Keselamatan dicatat dalam skala mulai dari 1-10, dengan 1 dianggap paling berbahaya dan 10 aman dan aman. Ini menentukan pos, video, benang dan teman mana yang

[21] http://webcache.googleusercontent.com/search?q=cache:wFNg1TLsYuEJ:bullyproofclassroom.com/technology-fight-cyberbullying+&cd=1&hl=id&ct=clnk&client=firefox-b diakses 17 Juni 2017, pukul 08.05 WIB

dianggap sesuai atau berisiko membahayakan reputasi anak.

(4) *STOPit*: Saat ini, hanya satu dari sepuluh korban *cyberbullying* yang menginformasikan orang dewasa tentang situasi mereka. Dengan aplikasi STOP, pengembang dan orang tua mencoba memberi anak tingkat kebebasan dan pemberdayaan yang lebih besar dengan memberi mereka alat untuk menghentikan penghentian penindasan di dunia maya itu sendiri. STOPit memungkinkan anak-anak mengambil tangkapan layar (*screenshot*) dari pelaku online berbahaya dan mengirimkannya ke pilihan orang dewasa yang disesuaikan, seperti guru dan orang tua. Sebagai contoh predator online yang lebih tua, anak-anak yang melaporkan masalah tetap anonim, dan aplikasinya menawarkan peringatan penegakan hukum lokal dan akses mudah ke jalur bantuan.

PENUTUP

A. Kesimpulan

Berdasarkan uraian tersebut diatas , dapat dikemukakan beberapa kesimpulan sebagai berikut: Kebijakan penang-gulangan *cyber bullying* dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan). Dilihat dari sudut *criminal policy*, upaya penanggulangan tindakan *cyber bullying* tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana *penal*), tetapi harus ditempuh pula dengan pendekatan integral/sistematik. Upaya penanggulangan *cyber bullying* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu, diperlukan pula pendekatan budaya/ kultural, pendekatan moral/edukatif, dan bahkan pendekatan global (kerja sama internasional).

B. 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 di-lakukan 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 PUSTAKA

Buku Literatur

Barda Nawawi Arief, 2008, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Prenada Media Group.

Barda Nawawi Arief, 2008, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penang-gulangan Kejahatan.*

Mahmud Mulyadi, 2008, *Criminal Policy: Pendekatan Integral Penal Policy dan Non-Penal Policy dalam Penanggulangan Kejahatan Kekerasan*, Medan: Pustaka Bangsa Press.

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

Mukhlis Ifransah, *"Perlindungan Hukum HKI di Era Digital",* hukumonline. com, Soedarto, 1981, *Hukum dan Hukum Pidana*, Bandung: Alumni.

Soedarto, 1981, *Kapita Selekta Hukum Pidana,*Bandung :Alumni.

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

Wahmuji, 2011, *Perihal Kejahatan dan Hukuman*, Yogyakarta: Genta Publishing,

Peraturan Perundang-undangan

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 TransaksiElektronik;

Sumber Internet

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

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

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

Lain-lain

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

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 BIdanDepkominfo, Jakarta, 10 Agustus 2006.

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

BIODATA SINGKAT PENULIS

Firda Laily Mufid, S.H., M.H., adalah Staf Pengajar pada Fakultas Hukum Universitas Islam Jember. Menyelesaikan pendidikan Sarjana (S1) pada Fakultas Hukum Universitas Jember dan Magister Ilmu Hukum (S2) Fakultas Hukum Universitas Jember.