KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN *CYBER CRIME* DI INDONESIA

SKRIPSI

Diajukan Guna Memenuhi Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Hukum (S.H.)
Program Studi Ilmu Hukum

Disusun Oleh :

MUHAMMAD MUIS
NPM. 1506200471

FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2019

MAJELIS PENDIDIKAN TINGGI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jl. Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6624-567 Medan 20238 Fax. (061) 662
Website : http://www.umsuac.id E-mail : rektor@umsu.ac.id
Bankir. Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

PENDAFTARAN UJIAN SKRIPSI

Pendaftaran Skripsi Sarjana Strata 1 Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, bagi:

NAMA	**: MUHAMMAD MUIS**
NPM	**: 1506200471**
PRODI/BAGIAN	**: ILMU HUKUM/HUKUM PIDANA**
JUDUL SKRIPSI	**: KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN *CYBER CRIME* DI INDONESIA**
PENDAFTARAN	**: 05 Oktober 2019**

Dengan diterimanya Skripsi ini, sesudah Lulus dari Ujian Skripsi Penulis berhak memakai gelar:

SARJANA HUKUM (S.H)

Diketahui
DEKAN FAKULTAS HUKUM

Dr. IDA HANIFAH, SH., M.H
NIP: 196003031986012001

PEMBIMBING

Dr. T. ERWINSYAHBANA, S.H., M.Hum
NIDN: 0006076814

MAJELIS PENDIDIKAN TINGGI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jl. Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6624-567 Medan 20238 Fax. (061) 662
Website : http://www.umsuac.id E-mail : rektor@umsu.ac.id
Bankir. Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA : **MUHAMMAD MUIS**
NPM : **1506200471**
PRODI/BAGIAN : **ILMU HUKUM/HUKUM PIDANA**
JUDUL SKRIPSI : **KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN *CYBER CRIME* DI INDONESIA**

Disetujui Untuk Disampaikan Kepada
Panitia Ujian

Medan, 02 Oktober 2019

DOSEN PEMBIMBING

Dr. T. ERWINSYAHBANA, S.H., M.Hum
NIDN: 0006076814

MAJELIS PENDIDIKAN TINGGI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jl. Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6624-567 Medan 20238 Fax. (061) 662
Website : http://www.umsuac.id E-mail : rektor@umsu.ac.id
Bankir. Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

BERITA ACARA
UJIAN MEMPERTAHANKAN SKRIPSI SARJANA
BAGI MAHASISWA PROGRAM STRATA I

Panitia Ujian Sarjana Strata I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam sidangnya yang diselenggarakan pada hari Rabu, Tanggal 09 Oktober 2019 Jam 08.30 WIB sampai dengan selesai, setelah mendengar, melihat, memperhatikan menimbang:

MENETAPKAN

NAMA	**: MUHAMMAD MUIS**
NPM	**: 1506200471**
PRODI/BAGIAN	**: ILMU HUKUM/HUKUM PIDANA**
JUDUL SKRIPSI	**: KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN *CYBER CRIME* DI INDONESIA**
Dinyatakan	**: (A) Lulus Yudisium dengan Predikat Istimewa** **( ) Lulus Bersyarat, Memperbaiki/Ujian Ulang** **( ) Tidak Lulus**

Setelah lulus, dinyatakan berhak dan berwenang mendapatkan gelar Sarjana Hukum (SH) dalam Bagian Pidana

PANITIA UJIAN

Ketua

Dr. IDA HANIFAH, SH., M.H
NIP: 196003031986012001

Sekretaris

FAISAL, SH., M.Hum
NIDN: 0122087502

ANGGOTA PENGUJI:

1. **AL- UMRY, S.H., M.Hum** 1.
2. **FAISAL RIZA, S.H., M.H** 2.
3. **Dr. T. ERWINSYAHBANA, S.H., M.Hum** 3.

MAJELIS PENDIDIKAN TINGGI MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jl. Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6624-567 Medan 20238 Fax. (061) 662
Website : http://www.umsuac.id E-mail : rektor@umsu.ac.id
Bankir. Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini :

Nama	: **MUHAMMAD MUIS**
NPM	: 1506200471
Program	: Strata – I
Fakultas	: Hukum
Program Studi	: Ilmu Hukum
Bagian	: Hukum Pidana
Judul Skripsi	: **KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN *CYBER CRIME* DI INDONESIA**

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis ini secara keseluruhan adalah hasil penelitian / karya saya sendiri. Kecuali bagian – bagian yang dirujuk sumbernya.

Dan apabila ternyata dikemudian hari skripsi ini merupakan hasil plagiat atau merupakan karya orang lain, maka dengan ini saya menyatakan bersedia menerima sanksi akademik dari Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Medan, Oktober 2019
Saya yang menyatakan

MUHAMMAD MUIS

ABSTRAK

KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANAN *CYBER CRIME* DI INDONESIA

Muhammad Muis

Globalisasi teknologi informasi yang telah mengubah dunia ke era *cyber* dengan sarana internet yang menghadirkan *cyberspace* dengan realitas virtualnya menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi di balik itu, timbul persoalan berupa kejahatan yang dinamakan *cyber crime*, kejahatan ini tidak mengenal batas wilayah (*borderless*) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. *cyber crime* dapat dilakukan melalui sistem jaringan komputernya itu sendiri yang menjadi sasaran dan komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. Perkembangan teknologi informasi yang demikian pesatnya haruslah diantisipasi dengan hukum yang mengaturnya. Dampak negatif tersebut harus diantisipasi dan ditanggulangi dengan hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Berdasarkan latar belakang permasalahan tersebut untuk melakukan penelitian terhadap Kebijakan Hukum Pidana dalam Penanggulangan *cyber crime* di Indonesia. Tujuan Penelitian ini untuk mengetahui kebijakan hukum pidana melalui pendekatan KUHP untuk menanggulangi tindak pidana *cyber crime* di Indonesia dan mengetahui kebijakan hukum pidana melalui UU ITE untuk menanggulangi *cyber crime* di Indonesia serta mengetahui penegakan hukum *cyber crime* di Indonesia secara penal dan non penal.

Penelitian ini bersifat yuridis normatif sebagai pendekatan utama, mengingat pembahasan didasarkan pada peraturan perundangundangan dan prinsip hukum yang berlaku dalam masalah kejahatan *cyber crime*. Pendekatan yuridis dimasudkan untuk melakukan pengkajian terhadap bidang hukum, khususnya hukum pidana.

Upaya penegakan hukum tidak hanya terbatas terhadap peningkatan kemampuan, sarana dan prasarana aparat penegak hukum tetapi juga diiringi kesadaran hukum masyarakat yang didukung dengan kerjasama dengan penyedia layanan internet.

Kata Kunci : Kebijakan Hukum Pidana , Penanggulangan, *Cyber Crime.*

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarkatuh

Yang pertama saya ucapkan rasa syukur kehadirat Allah SWT yang maha pengasih lagi penyayang atas segala rahmat dan karuniaNya sehingga skripsi ini dapat diselesaikan. Skripsi merupakan salah satu persyaratan bagi setiap mahasiswa yang ingin menyelesaikan studinya di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Sehubungan dengan itu, disusun skripsi yang berjudulkan "**KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN *CYBER CRIME* DI INDONESIA."**

Dengan selesainya skripsi ini, perkenankanlah saya mengucapkan rasa terimakasih yang sebesar-besarnya kepada: Rektor Universitas Muhammadiyah Sumatera Utara Bapak Dr. Agussani., M.AP atas kesempatan dan fasilitas yang diberikan kepada kami untuk mengikuti dan menyelesaikan pendidikan program Sarjana ini. Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Ibu Dr. Ida Hanifah, S.H., M.H atas kesempatan menjadi mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Demikian juga halnya kepada Wakil Dekan I Bapak Faisal, S.H., M. Hum dan Wakil Dekan III Bapak Zainuddin, S.H., M.H.

Terimakasih yang tak terhingga dan penghargaan yang setingi-tingginya diucapkan kepada Bapak T. Erwinsyahbana, S.H., M.Hum selaku Pembimbing yang dengan penuh perhatian telah memberikan dorongan, bimbingan dan arahan sehingga skripsi ini selesai.

Disampaikan juga penghargaan kepada seluruh staf pengajar Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Secara khusus dengan rasa hormat dan penghargaan yang setinggi- tingginya diberikan terima kasih kepada ayahanda dan ibunda: H. Mukti dan Hj. Siti Aisyah yang telah mengasuh dan mendidik dengan penuh curahan kasih sayang. Juga kepada saudara-saudara saya teruntuk para abang saya Razi Azmil dan Ma'in Yunus, serta para kakak saya yakni, Amira Lasari Am.Keb, Hj.Zaima S.E, dan Muzira Syahri BIAM yang telah mendukung saya sehingga saya mampu mencapai titik ini.

Tiada gedung yang paling indah, kecuali persahabatan, untuk itu, dalam kesempatan diucapkan terimakasih kepada sahabat-sahabat yang telah banyak berperan dalam keseharian saya yakni, untuk sahabat C-2 Siang, sahabat C-1 Pidana,dan Sahabat Komunitas Debat Hukum (KDH) . terimakasih, atas semua kebaikannya, semoga Allah SWT membalas kebaikan kalian. Kepada semua pihak yang tidak dapat disebutkan satu persatu namanya, tiada maksud mengecilkan arti pentingnya bantuan dan peran mereka, dan untuk itu disampaikan ucapan terimakasih yang setulus-tulusnya

Akhirnya, tiada gading yang tak retak, retaknya gading karena alami, tiada orang yang tak bersalah, kecuali Ilahi Rabbi. Mohon maaf atas segala kesalahan selama ini, begitupun disadari bahwa skripsi ini jauh dari sempurna. Untuk itu,

diharapkan ada masukan yang membangun untuk kesempurnaannya. Terima kasih semua, tiada lain yang diucapkan selain kata semoga kiranya mendapat balasan dari Allah SWT dan mudah-mudahan semuanya selalu dalam lindungan Allah SWT, Amin. Sesungguhnya Allah mengetahui akan niat baik hamba-hambanya.

Assalamu'alaikum Warahtnatullahi Wabarkatuh

Medan, Oktober 2019
Hormat Saya
Penulis,

Muhammad Muis
NPM 1506200471

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Penelitian

Kebijakan hukum pidana merupakan kebijakan dari negara melalui badan-badan yang berwenang untuk menerapkan peraturan-peraturan yang dikehendaki yang diperkirakan dapat digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan. Usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Jadi kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal. Di lihat dari sudut politik kriminal, maka politik hukum pidana identik dengan pengertian ”kebijakan penanggulangan kejahatan dengan hukum pidana”.

Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya merupakan bagian dari usaha penegakan hukum (khususnya penegakan hukum pidana). Politik hukum pidana merupakan bagian dari kebijakan penegakan hukum (*law enforcement policy*). Penggunaan upaya hukum termasuk hukum pidana, sebagai salah satu upaya mengatasi masalah sosial termasuk dalam bidang kebijaksanaan penegakan hukum. Disamping itu bertujuan mencapai kesejahteraan masyarakat pada umumnya, maka kebijaksanaan penegakan hukum ini pun termasuk dalam kebijaksanaan sosial, yaitu segala usaha yang rasional untuk mencapai kesejahteraan masyarakat.

Dalam hal kaitannya dengan kebijakan hukum pidana, salah satu bagian dari dimensi kehidupan sosial saat ini yang perlu kebijakan hukum pidana yakni dampak teknologi informasi yang sangat berkembang dengan pesat menyebabkan banyak perubahan pada segi kehidupan sosial masyarakat, baik ekonomi, sosial politik. Sistem komunikasi dan interaksi, pendidikan, termasuk juga hukum. Teknologi informasI, internet pada awalnya dikembangkan semata-mata untuk memudahkan manusia dalam menjalankan rutinitas kehidupannya.[1]

Teknologi informasi di yakini membawa keuntungan yang besar bagi negara-negara di dunia.[2] Lahir suatu rezim hukum baru yang dikenal dengan hukum *cyber*, yang diambil dari kata *Cyber Law* adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang digunakan yaitu Hukum Teknologi Informasi (*Law Of Information Technology*), Hukum Dunia Maya (*Virtual World Law*). Istilah-istilah tersebut lahir mengingat kegiatan internet dan manfaat teknologi informasi berbaris *virtual*. Istilah hukum *cyber* digunakan dalam tulisan ini dilandasi pemikiran bahwa *cyber* jika diidentikan dengan "Dunia Maya" akan cukup menghadapi persoalan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu.[3]

Perubahan paradigma ini juga diikuti perubahan cara pandangan baru. Cara pandang baru yang dimaksud adalah dokumentasi yang semula *paper based*

---

[1] Hardianto Djanggih," *Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan*". Jurnal Media Hukum. Vol.1 No.2, September 2013, halaman 57.

[2] Budi Suhariyanto. 2013. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Depok : PT. Rajagrafindo Persada, halaman 1.

[3] *Ibid*. halaman 2.

menjadi *electronic based*. Hal ini menjadi sangat jelas ketika melakukan transaksi lewat pasar *online* (internet). Dalam transaksi ini akan terlihat bahwa keseluruhannya serba berbasis elektronik, misalnya *digital signature*, *e-mail*. Teknologi informasi (*information technology*) membawa dampak bagi masyarakat secara luas, baik dampak positif maupun negatif. Dampak positifnya adalah dapat memperoleh berbagai informasi, baik dari dalam maupun luar negeri , transaksi jarak jauh. Sedangkan dampak negatifnya adalah memberikan peluang untuk melakukan berbagai kejahatan, seperti penipuan, pencurian, pencemaran nama baik, keasusilaan, perjudian, pengancaman, perusakan dan teror yang seluruhnya dikenal dengan *cyber crime.*

Cyber crime adalah kejahatan yang dilakukan oleh seseorang, sekelompok orang dan korporasi (badan hukum) dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer. Kejahatan ini terjadi di dunia maya (*virtual*) sehingga mempunyai karakteristik yang berbeda dengan kejahatan tradisional.

Berdasarkan beberapa hasil penelitian, karakteristik pelaku *cyber crime* sangat unik, dan juga berbeda kategori dengan pelaku kejahatan lain. Meskipun hukum pidana konvensional sebagaimana yang berlaku di Indonesia dapat digunakan hakim sebagai dasar hukum untuk mengadili pelaku *cyber crime*, akan tetapi dalam praktik sangat banyak keterbatasannya, baik dari sisi unsur tindak pidana maupun pertanggungjawaban pidananya. Akibatnya, banyak pelaku yang lolos dari jeratan hukum. Berdasarkan hasil penelitian yang dilakukan oleh Widodo dalam "Sistem Pemidanaan dalam *Cyber Crime*" semua pelaku dijatuhi

pidana penjara. Dalam tataran filosofis, teoritis, normatif maupun empiris, pidana penjara merupakan suatu jenis pidana yang mempunyai banyak kelemahan karena pelaksanaan pidana penjara khususnya di Indonesia kurang memadai.

Kejahatan baru ini sangat berdampak pada dunia usaha. Banyak yang menganggap bahwa keberadaan KUHP tidak mampu menjangkau kejahatan baru tersebut, sehingga pemerintah menginisiasi lahirnya aturan tentang *cyber crime.* Berdasarkan dokumen yang ada, Undang-Undang Tentang Informasi dan Trsansaksi Elektonik (UU ITE) yaitu Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008.

Menurut Widodo, penjatuhan pidana penjara para pelaku *cyber crime* adalah langkah yang kurang bijak. Hal ini disebabkan oleh ketidaksesuaian antara karakteristik pelaku tindak pidana dengan sistem pembinaan narapidana di Lembaga Pemasyarakatan, sehingga tujuan pemidanaan sebagaimana diatur dalam Undan-Undang Pemasyarakatan tidak akan tercapai. Menurut Widodo, sebagai pengganti pemidanaan tersebut adalah pidana kerja sosial atau pidana pengawasan.[4]

Karena ada kesesuaian antara karakteristik pelaku *cyber crime* dengan paradigma pemidanaan dalam pidana kerja sosial atau pidana pengawasan, sehingga tujuan pemidanaan dapat dicapai.[5] Sejalan dengan pandangan Widodo, dalam mengantisipasi *cyber crime*, Rancangan Undang-Undang Kitab Undang-

---

[4] Widodo. 2013 . "*Sistem Pemidanaan dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime",*Yogyakarta: Laksbang Mediatama,halaman3

[5] Pidana kerja sosial dan pidana pengawasan termasuk jenis-jenis pemidanaan yang tercantum dalam RUU KUHP Tahun 2007 pada Pasal 65 ayat 1.

Undang Hukum Pidana (RUU KUHP) mencoba memperluas cakupan istilah untuk dapat membidik dan menjaring kejahatan tersebut.[6]

Sedangkan menurut Barda Nawawi Arief, dalam perspektif hukum pidana, upaya penanggulangan *cyber crime* dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggung–jawaban pidana atau pemidanaan (termasuk aspek pembuktian dan alat bukti), dan aspek yurisdiksi.[7] Berkaitan dengan hal tersebut, perumusan tindak pidana di dalam KUHP masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cyber crime*. Di samping itu, mengandung berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan *hitech crime* (kejahatan berteknologi tinggi) yang sangat bervariasi. Misalnya, untuk menghadapi masalah pemalsuan kartu kredit dan transfer dana elektronik, dalam KUHP tidak ada ketentuan khusus mengenai pembuatan kartu kredit, yang ada hanya ketentuan mengenai; sumpah/keterangan palsu tercantum pada Bab IX Pasal 242 KUHP, pemalsuan mata uang dan uang kertas pada Bab X Pasal 244-252 KUHP, tentang pemalsuan pada Bab XI Pasal 253-262 KUHP, pemalsuan surat pada Bab XII Pasal 263-276 KUHP.[8]

Indonesia mencoba melakukan kebijakan harmonisasi dengan negara-negara lain, khususnya dalam lingkungan Asia dan Asean menyangkut masalah *cyber crime.* Antisipasi masalah *cyber crime* tidak hanya melalui Undang-Undang

---

[6] *Ibid*.halaman3.

[7] Barda Nawawi Arief. 2005 .*Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan* , Bandung: Pranamedia Group,halaman 125

[8] *Ibid*.halaman 127-128

Informasi dan Transaksi Elektronik (UU ITE), namun juga berusaha mengantisipasinya dalam penyusunan RUU KUHP.

Dalam Buku I RUU KUHP Indonesia pada Pasal 174 dalam Ketentuan Umum, disebutkan tentang pengertian "barang", yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon, telekomunukasi, atau jasa komputer. Adapun redaksi teks Pasal 174 sebagai berikut:

"Barang adalah benda berwujud termasuk air dan uang giral, dan benda tidak berwujud termasuk aliran listrik, gas, data dan program komputer, jasa telepon, jasa telekomunikasi, atau jasa komputer".[9]

Dalam Buku I RUU KUHP Indonesia Pasal 188 juga dicantumkan tentang pengertian "surat", mencakup data tertulis atau tersimpan dalam disket, pita magnetik, media penyimpan komputer atau penyimpan data elektronik lainnya. Dalam pasal tersebut dinyatakan:

"Surat adalah selain surat yang tertulis di atas kertas, juga surat atau data yang tertulis atau tersimpan dalam disket, pita magnetik, atau media penyimpan komputer atau media penyimpan data elektronik lain"[10]

Definisi "surat" menggambarkan makna surat secara berwujud (tertulis) dan tidak berwujud *(virtual).* Makna surat yang tidak berwujud dapat berupa *e-mail*, *massage* dalam *chatting/guest book situs*, komentar tertulis dalam sebuah situs dalam bentuk aplikasi apapun, *short massage service* (SMS) atau *Whatsaap* (WA), termasuk di dalamnya *software* (perangkat lunak). Berdasarkan 2 (dua)

[9] Barda Nawawi Arief, op. cit., halaman 131
[10] *Ibid.* halaman 135

pasal tersebut, dapat menjadi gambaran untuk melihat *cyber crime* dari sudut pandang RUU KUHP. Hal ini dimaksudkan untuk mencegah dan mengurangi kejahatan yang terjadi dalam dunia maya. Selain itu, agar pelaku kejahatan yang berkaitan dengan kemajuan berteknologi dapat dijerat dengan undang-undang tersebut.

Aspek pokok aktivitasnya, *cyber crime* dilakukan lebih menitikberatkan pada penyerangan *content, computer system* dan *communication system* milik orang lain, baik secara personal maupun umum di dalam *cyber space*. Untuk itu, diperlukan pengamanan sebuah sistem untuk mencegah terjadinya perusakan. Penanggulangan *cyber crime* dilakukan dengan pencegahan dan penegakan hukum, demi tercapainya supremasi hukum. Apabila dibiarkan terus menerus, dapat mengganggu keamanan baik secara nasional maupun internasional. Sesungguhnya *cyber crime* sudah mengganggu keamanan dalam negeri maupun luar negeri, sehingga diperlukan langkah-langkah strategis aparat penegak hukum untuk menanggulanginya.[11]

Cyber crime terjadi karena kontrol personal dan kontrol sosial lemah. Hal ini disebabkan karena kejahatan ini bersifat maya (*virtual)*, ketika pelaku tidak tampak secara fisik. Dalam pendekatan normatif, *cyber crime* ini ada yang merupakan kejahatan konvensional tetapi dengan modus baru seperti, pornografi, penipuan, pencemaran nama baik dan sebagainya, yang menggunakan media

[11] *Cyber crime* bersifat nyata (*real*) tetapi maya (*virtual*) adalah kenyataan suatu peristiwa hukum yang terjadi dalam ruang maya (*cyber space*) atau internet. Secara yuridis aktivitas tersebut tidak dapat dideteksi dengan ukuran dan kualifikasi hukum konvensional, karena apabila cara ini yang ditempuh akan banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Oleh karena itu, hal ini perlu dilengkapi fasilitas aturan hukum yang serupa dan sepadan. Seperti halnya Undang-Undang RI Nomor 11 Tahun 2008 tentang ITE yang mencoba menjangkau ruang maya tersebut.

internet sebagai sarana untuk melakukan kejahatan, maka dapat dipidana dengan melihat Kitab Undang-Undang Hukum Pidana (KUHP), sementara itu terhadap *cyber crime* jenis baru seperti *hacking*, kejahatan ini tidak ada ketentuan dalam KUHP. Dengan demikian terjadi kekosongan hukum (*rechts vacuum*).[12]

Lahirnya Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) telah dinilai mampu mengakomodir jenis kejahatan yang merupakan pengembangan terhadap kejahatan melalui media internet. Selain itu, undang-undang tersebut diharapkan menjadi jawaban konkrit terhadap masalah yang dihadapi oleh aparatur penegak hukum.[13]

Dengan demikian *cyber crime* adalah tindakan yang dilarang oleh Allah swt, karena Allah swt. tidak menyukai orang-orang yang membuat kerusakan yang memudharatkan orang lain. Perusakan dalam bentuk apapun tidak dibenarkan, karena perusakan merupakan tindakan yang bertentangan dengan nilai-nilai universal. Allah swt. secara tegas berfirman dalam Q.S. Al-Maidah/5: 64 sebagai berikut:

وَقَالَتِ ٱلۡيَهُودُ يَدُ ٱللَّهِ مَغۡلُولَةٌۚ غُلَّتۡ أَيۡدِيهِمۡ وَلُعِنُواْ بِمَا قَالُواْۘ بَلۡ يَدَاهُ مَبۡسُوطَتَانِ يُنفِقُ كَيۡفَ يَشَآءُۚ وَلَيَزِيدَنَّ كَثِيرٗا مِّنۡهُم مَّآ أُنزِلَ إِلَيۡكَ مِن رَّبِّكَ طُغۡيَٰنٗا وَكُفۡرٗاۚ وَأَلۡقَيۡنَا بَيۡنَهُمُ ٱلۡعَدَٰوَةَ وَٱلۡبَغۡضَآءَ إِلَىٰ يَوۡمِ ٱلۡقِيَٰمَةِۚ كُلَّمَآ أَوۡقَدُواْ نَارٗا لِّلۡحَرۡبِ أَطۡفَأَهَا ٱللَّهُۚ وَيَسۡعَوۡنَ فِي ٱلۡأَرۡضِ فَسَادٗاۚ وَٱللَّهُ لَا يُحِبُّ ٱلۡمُفۡسِدِينَ ٦٤

[12] Nia Kurnia dalam http://student *research student umm.ac.id// department _off_syariah /article/view/ 7253/0* (diakses pada tanggal,18 juli 2019).

[13] Undang-Undang Republik Indonesia No. 19 Tahun 2019 tentang Informasi dan Transaksi Elektronik (ITE) selanjutnya disebut Undang-Undang ITE

Terjemahnya:
"Dan orang-orang Yahudi berkata: "Tangan Allah terbelenggu". Sebenarnya tangan merekalah yang dibelenggu dan merekalah yang dilaknat disebabkan apa yang telah mereka katakan itu. Padahal kedua tangan Allah terbuka; Dia memberi rezki sebagaimana dia kehendaki. Dan (Alquran) yang diturunkan kepadamu dari Tuhanmu itu pasti akan menambah kedurhakaan dan kekafiran bagi kebanyakan mereka. Dan Kami timbulkan permusuhan dan kebencian di antara mereka sampai hari kiamat. Setiap mereka menyalakan api peperangan, Allah memadamkannya dan mereka berbuat kerusakan dimuka bumi dan Allah tidak menyukai orang-orang yang membuat kerusakan."

Ayat tersebut menegaskan bahwa tindakan perusakan merupakan sesuatu yang dilarang oleh Allah swt. baik dalam bentuk apapun dan di manapun, tetap tidak dibenarkan. Tindakan para *hacker* menjadi bagian dari perbuatan dan tindakan yang sangat dominan dilakukan oleh para pelaku kejahatan *cyber crime* yang dilarang sebagaimana ayat tersebut. Landasan larangan tersebut mengarah kepada hal-hal yang merugikan dan meresahkan orang lain.

Berdasarkan latar belakang masalah yang telah diuraikan diatas mendorong penulis untuk melakukan penelitian dengan judul **"KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANAN *CYBER CRIME* DI INDONESIA".**

1. **Rumusan Masalah**

Berdasarkan latar belakang masalah yang telah diuraikan di atas maka penulis mengidentifikasikan masalah-masalah yang akan menjadi pokok pembahasan yaitu:

a. Bagaimanakah kebijakan hukum pidana dalam penanggulangan *cyber crime* di indonesia ?

b. Bagaimanakah penegakan hukum *cyber crime* di indonesia melaui sarana penal dan non penal ?

c. Bagaimanakah faktor – faktor yang mempengaruhi dalam penanggulangan *cyber crime* di Indonesia ?

2. Faedah Penelitian

Merujuk pada rumusan masalah yang akan diteliti sebagaimana disebutkan diatas, penelitian ini diharapkan dapat memberikan faedah sebagai berikut:

a. Secara teoritis penelitian ini diharapkan dapat menjadi salah satu sumber atau bahan pembelajaran bagi msayarakat terkait tindakan hukum pidana mengenai *cyber crime.*

b. Secara praktis sebagai bentuk sumbangan saran sebagai buah pemikiran bagi pihak yang berkepentingan dalam kerangka persoalan penerapan kebijakan tindak terhadap penanggulangan *cyber crime*

B. Tujuan Penelitian

Tujuan penelitian harus tergambar secara tegas apa yang hendak dicapai di dalam melaksanakan penelitian tersebut. Tujuan penelitian harus bertitik tolak dari permasalahan. Bahkan harus terlibat tegas jika permasalahan ada 3 (tiga) maka tujuan penelitian harus 3 (tiga).Ketika hal tersebutlah yang menjadi pokok permasalahan yang intisarinya harus terlihat pada kesimpulan.

Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Untuk mengetahui kebijakan hukum pidana yang efisien dan praktis dalam penanggulangan tindak pidana *cyber crime* di indonesia.

2. Untuk mengetahui langkah penegakan hukum yang tepat terkait *cyber crime* di indonesia melaui sarana penal dan non penal.
3. Untuk mengetahui faktor–faktor yang mempengaruhi dalam penanggulangan tindak pidana *cyber crime* di indonesia.

C. Metode Penelitian

Metodologi merupakan suatu unsur yang muthlak yang harus ada di dalam penelitian dan pengembangan ilmu pengetahuan. Istilah "*metodologi"* berasal dari kata "metode" yang berarti "jalan ke". Terhadap pengertian metodologi, biasanya diberikan arti-arti sebagai logika dari penelitian ilmiah, studi terhadap prosedur dan teknik penelitian.[14] Agar mendapatkan hasil yang maksimal, maka metode yang dipergunakan dalam penelitian ini terdiri dari:

1. Jenis penelitian

Jenis penelitian yang digunakan adalah penelitian hukum yuridis normatif yang menganalisis permasalahan berdasarkan perundang-undangan yang berlaku dan juga literatur yang membahas permasalahan yang ditinjau.

2. Pendekatan penelitian

Pendekatan melalui Undang-Undang, yakni pendekatan yang dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang diteliti.

3. Sifat penelitian

Berdasarkan judul penelitian dan rumusan masalah, sifat penelitian yang dilakukan termasuk dalam kategori penelitian deskriptif adalah penelitian hanya

[14] Soerjono Soekanto. 2014 . *Pengantar Penelitian Hukum* . Jakarta : UI-Press. 2014. halaman 67.

semata-mata melukiskan keadaan objek atau peristiwa tanpa suatu maksud untuk mengambil kesimpulan-kesimpulan secara umum.

4. Sumber data

Sumber data yang dapat digunakan dalam melakukan penelitian hukum ini yaitu :

a. Data yang bersumber dari hukum Islam; yaitu Al-Qur'an dan Hadist (Sunah Rasul). Data yang bersumber dari Hukum Islam tersebut lazim disebut pula sebagai kewahyuan.
b. Selanjutnya sumber data yang digunakan adalah data sekunder, dimana data sekunder tersebut mencakup :
c. Bahan hukum primer yaitu bahan-bahan hukum yang mengikat. Dalam penelitian ini, bahwa hukum primer yang digunakan peraturan perundang-undangan seperti Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP)
d. Bahan hukum sekunder yaitu yang memberikan penjelasan mengenai bahan hukum primer. Bahan hukum sekunder berupa semua publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi. Publikasi tentang hukum meliputi buku-buku yang terkait dengan masalah yang dikaji, hasil penelitian, jurnal, hasil karya dari kalangan hukum.
e. Bahan hukum tersier yaitu bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder

berupa kamus hukum atau kamus bahasa Indonesia untuk menjelaskan maksud atau pengertian istilah-istilah yang sulit untuk diartikan.[15]

5. Alat pengumpul data

Mengingat penelitian ini adalah penelitian yang bersifat yuridis normatif yang memusatkan perhatian pada data sekunder, maka pengumpulan data utama di tempuh dengan melakukan penelitian kepustakaan dan studi dokumen-dokumen yang berakitan dengan rumusan masalah.

6. Analisis data

Data yang terkumpul tersebut akan dianalisa dengan seksama dengan menggunakan analisis kualitatif yakni pemilihan teori-teori, asas-asas, norma-norma, doktrin dan pasal-pasal dalam undang-undang yang relevan dengan permasalahan, membuat sistematika dari data-data tersebut sehingga akan menghasilkan kualifikasi tertentu yang sesuai dengan permasalahan yang akan dibahas dalam penelitian ini. Data yang dianalisis secara kualitatif akan dikemukakan dalam uraian secara sistematis pula, selanjutnya semua data diseleksi, diolah kemudian dinyatakan secara deskriptif sehingga dapat memberikan seleksi terhadap permasalahan yang dimaksud.

D. Definisi Operasional

Definisi operasional atau kerangka konsep adalah kerangka yang menggambarkan hubungan antara definisi-definisi atau konsep-konsep khusus yang akan diteliti. Konsep merupakan salah satu unsur konkrit dari teori namun demikian, masih diperlukan penjabaran lebih lanjut dari konsep ini dengan jalan

---

[15] *Ibid.*halaman 52.

memberikan definisi operasionalnya Beberapa definisi operasional yang telah ditentukan antara lain:

1. Kebijakan hukum pidana dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah (termasuk penegak hukum) dalam mengelola, mengatur atau menyelesaikan urusan-urusan publik, masalah-masalah masyarakat atau bidang-bidang penyusunan peraturan perundang-undangan dan mengalokasikan hukum/peraturan dalam suatu tujuan (umum) yang mengarah pada upaya mewujudkan kesejahtraan dan kemakmuran masyarakat (Warga Negara).

   Istilah politik hukum pidana ini juga disebut *penal policy*, *criminal law policy* atau *strafrechts politiek Hukum* adalah sistem yang terpenting dalam pelaksanaan atas rangkaian kekuasaan kelembagaan[16]
2. Kebijakan penanggulangan *cyber crime* merupakan bagian dari *criminal policy*. Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cyber crime*) tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus pula ditempuh dengan pendekatan integral. Operasionalisasi kebijakan penal meliputi kriminalisasi, dekriminalisasi, penalisasi dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial. Oleh karena itu, penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu

[16] Wikipedia, "Hukum" https://id.wikipedia.org/wiki/Hukum, diakses Kamis, 15 juli 2019, Pukul 19.10 wib.

perilaku sosial. Sebagai salah satu bentuk *high tech crime* yang dapat melampaui batas-batas negara (bersifat *transnational/transborder*), merupakan hal yang wajar jika upaya penanggulangan *cyber crime* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu, diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan pendekatan global melalui kerjasama internasional.

3. *Cyber Crime* merupakan segala macam penggunaan jaringan komputer untuk tujuan kriminal atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.[17] *Cyber crime* dapat dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana / alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Kejahatan komputer yang diasosiasikan dengan *hacker*, biasanya menimbulkan arti yang negatif.

E. Jadwal Penelitian

Untuk melaksanakan penelitian yang direncanakan, maka penelitian ini akan dijadwalkan sebagai berikut :

1. Tahap persiapan

Pada tahapan ini dilakukan persiapan dalam urusan administrasi pengajuan judul, pencarian data-data awal untuk pembuatan dan pengajuan judul

[17] Abdul Wahid dan Mohammad Labib. 2015 . *kejahatan Mayantara (cyber crime).* Jakarta : PT Refika Aditama , halaman 103.

skripsi, dan penyusunan proposal skripsi dibutuhkan waktu 3 (tiga) minggu.

2. **Tahap pengumpulan data**

   Pada tahapan ini dilakukan pengumpulan bahan-bahan primer, pengumpulan bahan-bahan sekunder, dan pengumpulan bahan-bahan tersier, untuk menunjang penulisan proposal skripsi dibutuhkan waktu 2 (dua) minggu.

3. **Tahap pengelolaan data**

   Dalam tahap ini dilakukan pengelolaan serta penyempurnaan terhadap semua data yang diperoleh untuk memecahkan permasalahan dan menarik kesimpulan hasil penelitian, diperlukan waktu 4 (empat) minggu.

4. **Tahap penyelesaian**

   Tahap ini merupakan tahap akhir pada rangkaian penelitian skripsi dan pemeriksaan hasil skripsi oleh dosen pembimbing diperlukan waktu 3 (tiga) minggu.

BAB II

TINJAUAN PUSTAKA

A. Pengertian Kebijakan Hukum Pidana

Istilah kebijakan berasal dari bahasa Inggris *policy* atau dalam bahasa Belanda *politie*. 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 hukum/peraturan, dengan suatu tujuan yang mengarah.

Upaya perlindungan masyarakat (*social defence*) dan upaya mencapai kesejahteraan masyarakat (*social welfare*) pada hakikatnya merupakan bagian integral dari kebijakan atau upaya penanggulangan kejahatan .[18]

Pengertian kebijakan atau politik hukum pidana dapat dilihat dari politik hukum maupun politik kriminal. Menurut Sudarto, "Politik Hukum" adalah :

1. Usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat
2. Kebijakan dari negara melalui badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan. [19]

---

[18]Barda Nawawi Arief, Bunga Rampai . 2013 . *Kebijakan Hukum Pidana*, Bandung : Citra Aditya Bakti . halaman 32.

[19]Sudarto. 2012 . *Hukum dan Hukum Pidana*, Jakarta : Rajawali pers . halaman 44-48.

Bertolak dari pengertian demikian Sudarto selanjutnya menyatakan, bahwa melaksanakan "politik hukum pidana" berarti mengadakan pemilihan untuk mencapai hasil perundang-undangan pidana yang paling baik dalam arti memenuhi syarat keadilan dan daya guna.

Dalam kesempatan lain beliau menyatakan, bahwa melaksanakan "politik hukum pidana" berarti, "usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang. Dengan demikian, dilihat sebagai bagian dari politik hukum, maka politik hukum pidana mengandung arti, bagaimana mengusahakan atau membuat dan merumuskan suatu peraturan perundang-undangan pidana yang baik. Menurut Mahmud Mulyadi, politik hukum pidana merupakan upaya menentukan kearah mana pemberlakuan hukum pidana indonesia di masa yang akan datang dengan melihat penegakkannya saat ini.

Pengertian demikian terlihat pula dalam definisi "*penal policy*" dari Marc Ancel yakni "suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik". Melihat dari uraian di atas yang dimaksud dengan "peraturan hukum positif" (*the positive rules*) dalam definisi Marc Ancel itu jelas adalah peraturan perundangundangan dengan hukum pidana. Dengan demikian, istilah "*penal policy*" menurut Marc Ancel adalah sama dengan istilah "kebijakan atau politik hukum pidana" yang dikemukakan oleh Sudarto.

Melihat penjelasan di atas dapat ditegaskan, bahwa pembaharuan hukum pidana (*penal reform*) merupakan bagian dari kebijakan/politik hukum pidana

(*penal policy*). Latar belakang diadakannya pembaharuan hukum pidana dapat ditinjau dari aspek sosiopolitik, sosiofilosofis, sosiokultural, atau dari berbagai aspek kebijakan khususnya kebijakan sosial, kebijakan kriminal, dan kebijakan penegakan hukum. Artinya, pembaharuan hukum pidana pada hakikatnya harus merupakan perwujudan dari perubahan dan pembaruan terhadap berbagai aspek dan kebijakan yang melatarbelakangi pembaharuan tersebut.

Menurut Moeljatno, hukum pidana adalah bagian dari keseluruhan hukum yang berlaku disuatu negara yang mengadakan dasar-dasar dan aturan aturan untuk :

1. Menentukan perbuatan-perbuatan mana yang tidak boleh dilakukan, yang dilarang, dengan disertai ancaman atau sanksi yang berupa pidana tertentu bagi yang telah melanggar larangan tersebut;
2. Menentukan kapan dan dalam hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenakan atau dijatuhi sanksi pidana sebagaimana yang telah diancamkan.
3. Menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut. [20]

Menurut C. S. T. Kansil, hukum pidana adalah peraturan atau hukum yang mengatur tentang pelanggaran-pelanggaran dan kejahatan-kejahatan terhadap kepentingan umum, dan bagi pelanggarnya diancam dengan hukuman yang merupakan suatu penderitaan dan siksaan dengan tujuan untuk menimbulkan efek

[20] Raharjo, Agus . 2002 . *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* .Bandung: PT Citra Aditya Bakti. halaman 132.

jera pada penerima sanksi tersebut. Mengenai penentuan suatu perbuatan pidana, hukum Indonesia menganut asas legalitas yakni suatu perbuatan tidak dapat dihukum selain atas kekuatan aturan pidana dalam undang-undang, yang diadakan sebelum perbuatan itu terjadi (Pasal 1 ayat (1) KUHP). Hal ini dirumuskan oleh Anselm Von Feuderbach sebagai berikut:

"Nulla Poena Sinelege"

"Nulla Poena sine crimine"

"Nullum crimen sine poena legali "

Artinya:

"Tidak ada hukuman, kalau tidak ada undang-undang"

"Tidak ada hukuman, kalau tak ada kejahatan"

"Tidak ada kejahatan, kalau tidak ada hukuman yang berdasarkan undang-undang".[21]

B. Pengertian Kebijakan Penanggulangan *Cyber Crime*

Kebijakan penanggulangan *cyber crime* dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan).[22] Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cyber crime*) tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus pula ditempuh dengan pendekatan integral/sistemik

Sebagai salah satu bentuk *high tech crime* yang dapat melampaui batas-batas negara (bersifat *transnational/transborder*), merupakan hal yang wajar jika

[21] Abdulla Wahid. Dkk. 2005. *Kejahatan Mayantara (Cyber Crime)* .Bandung : Refika Aditamag . halaman 74 .

upaya penanggulangan *cyber crime* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu, diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan pendekatan global melalui kerjasama internasional.

Operasionalisasi kebijakan penal meliputi kriminalisasi, dekriminalisasi, penalisasi dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial. Oleh karena itu, penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu perilaku sosial.

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana. Jadi pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana sehingga itu termasuk bagian dari kebijakan hukum pidana (*penal policy*), khususnya kebijakan formulasi.

Menurut Bassiouni, keputusan untuk melakukan kriminalisasi dan dekriminalisasi harus didasarkan pada faktor-faktor kebijakan tertentu yang mempertimbangkan bermacam-macam faktor, termasuk:

1. Keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil-hasil yang ingin dicapai;
2. Analisis biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari.

3. Penelitian atau penafsiran tujuan-tujuan yang dicari itu dalam kaitannya dengan prioritas lainnya dalam pengalokasian sumber-sumber tenaga manusia.
4. Pengaruh sosial dari kriminalisasi dan dekriminalisasi yang berkenaan dengan pengaruh-pengaruhnya yang sekunder.[23]

Kebijakan Penangggulangan *cyber crime* hukum dalam pidana di Indonesia selama ini dapat diidentifikasikan sebagai berikut :

1. Dalam KUHP

Perumusan tindak pidana di dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cyber crime*, selain itu juga terdapat berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan *high tech crime* yang sangat bervariasi. Contoh dalam hal menghadapi masalah pemalsuan kartu kredit dan transfer dana elektronik saja, KUHP mengalami kesulitan karena tidak adanya aturan khusus mengenai hal tersebut. Ketentuan yang ada hanya mengenai :

a. sumpah/keterangan palsu (Pasal 242)
b. pemaluan mata uang dan uang kertas (Pasal 244-252)
c. pemalsuan materai dan merk (Pasal 253-262)
d. pemalsuan surat (Pasal 263-276).

2. Undang-undang di luar KUHP
    a. UU No.36 Tahun 1999 tentang Telekomunikasi, mengancam pidana terhadap perbuatan:

[23] *Ibid.* halaman 32

b. memanipulasi akses ke jaringan telekomunikasi (Pasal 50 jo.22)
c. menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi (Pasal 55 jo.38)
d. menyadap informasi melalui jaringan telekomunikasi (Pasal 56 jo.40).
e. Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan Atas UU No.31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi; Pasal 38 UU No.15 Tahun 2002 tentang Tindak Pidana Pencucian Uang; dan pasal 44 ayat (2) UU No.30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi; mengakui *electronic record* sebagai alat bukti yang sah.; UU No.32 Tahun 2002 tentang Penyiaran, antara lain mengatur tindak pidana:
    1) Pasal 57 jo. 36 ayat (5) mengancam pidana terhadap siaran yang :
        a) bersifat fitnah, menghasut, menyesatkandan/atau bohong;
        b) menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang; atau
        c) mempertentangkan suku, agama, ras, dan antar golongan.
    2) Pasal 57 jo. 36 ayat (6) mengancam pidana terhadap siaran yng memperolokkan,merendahkan, melecehkan, dan/atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasional.
    3) Pasal 58 jo. 46 ayat (3) Mengancam pidana terhadap siaran iklan niaga yang didalamnya memuat:
        a) promosi yang dihubungkan dengan ajaran suatu agama

Kriminalisasi *cyber crime* di Indonesia khususnya dalam UU ITE dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatan-perbuatan yang menjadikan komputer sebagai sasaran kejahatan. Kejahatan yang menggunakan komputer sebagai sarana adalah setiap tindakan yang mendayagunakan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukan kejahatan di ruang maya bukan ruang nyata. Kejahatan yang menjadikan komputer sebagai sasaran adalah setiap perbuatan dengan menggunakan komputer yang diarahkan pada data komputer, sistem komputer, atau jaringan komputer, atau ketiganya secara bersama-sama. Perbuatan tersebut dilakukan di ruang maya bukan ruang nyata, sehingga seluruh aktivitas yang dilarang oleh peraturan perundangundangan terjadi di ruang maya.[24]

Menurut Andi Hamsa dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" 2013 mengartikan *cyber crime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara *ilegal*. Forester dan Morrison mendefinisikan kejahatan komputer sebagai senjata utama, sedangkan Girasa (2013) mendefinisikan *cyber crime* sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama. Disamping itu, M.Yoga (2013) memberikan definisi *cyber crime* yang lebih menarik, yaitu kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi siber dan terjadi di dunia siber.

[24] Abdul Manan. 2013 . *Aspek –Aspek Pengubah Hukum*. Jakarta : Kencana . halaman 66.

Menurut John R.B menyatakan bahwa *brainware* adalah tenaga manusia yang mengatur proses dan yang mengoperasikan komputer, Contohnya *programmer*, *operator*, dan *user* menyebutkan bahwa orang yang paling sering dijaga tentang privasi mereka adalah ketika mereka tidak memiliki kepercayaan pada orang lain. Hampir semua definisi kepercayaan terlibat minimal dua agen yaitu orang yang harus percaya dan orang yang dipercaya. Penerapan teknologi baru tidak dapat terjadi tanpa minimum tingkat kepercayaan dalam perangkat dan para agen yang menjaga dan mengoperasikannya. Mereka menegaskan bahwa pengguna dengan kemampuan internet yang lebih besar dan tahun penggunaan biasanya memiliki kepercayaan lebih dalam terhadap internet.

Tindak pidana *cyber crime* memakan korban yang tidak sedikit jumlahnya, terutama dari sisi finansial. Sebagian besar korban hanya bisa menyesali apa yang sudah terjadi. Mereka berharap bisa belajar banyak dari pengalaman yang ada, yang perlu dilakukan sekarang adalah melakukan pencegahan terhadap kemungkinan-kemungkinan yang dapat merugikan kita sebagai pelaku IT. Pencegahan itu dapat berupa :

1. *Educate User* (memberikan pengetahuan baru terhadap *Cyber Crime* dan dunia internet)
2. *Use hacker's perspective* (menggunakan pemikiran dari sisi *hacker* untuk melindungi sistem Anda)
3. *Patch System* (menutup lubang-lubang kelemahan pada sistem)
4. *Policy* (menentukan kebijakan-kebijakan dan aturan-aturan yang melindungi sistem Anda dari orang-orang yang tidak berwenang)

5. *IDS (Intrusion Detection System) bundled with IPS (Intrusion Prevention System).*[25]

C. Pengertian *Cyber Crime*

Istilah *cyber crime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya *(cyber space*) dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindak kejahatan *cyber* (*cyber crime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan diantara keduanya. Beberapa penggunaan kata untuk merujuk pada *cyber crime* yang umum digunakan dalam berbagai literatur adalah kejahatan dunia maya, kejahatan komputer, kejahatan mayantara, kejahatan dibidang teknologi informasi, dan masih banyak lagi.[26]

konsep hukum *cyber space*, *cyber law*, dan *cyber line* yang dapat menciptakan komunitas pengguna jaringan internet yang luas 60 juta, yang melibatkan 160 negara menimbulkan kegusaran para praktisi hukum untuk menciptakan pengamanan melalui regulasi, khususnya perlindungan terhadap milik pribadi.[27]

Didik M. Arief Mansur dan elisatris Gultom dalam bukunya "*cyber law* aspek hukum teknologi informasi" menyebutkan secara umum yang dimaksud dengan kejahatan komputer atau kejahatan di dunia maya adalah : "perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut"[28]

---

[25]Wahid, Abdul. 2014. *Kejahatan Mayantara (Cyber Crime).* PT Refika Aditama. Bandung . halaman 78.

[26] *Ibid.*halaman 3-4.

[27]Suparni, Neniek . 2012 . *Cyber Space Problematika & Antisipasi Pengaturannya*. Sinar Grafika. Jakarta.halaman 48.

[28] *Ibid,*halaman 5.

Barda Nawawi Arief menunjuk pada kerangka (sistematik) Draf *Convention on Cyber Crime* dari dewan eropa (Draf No. 25, Desember 2000). Beliau menyamakan peristilahan antara keduanya dengan memberikan defenisi *cyber crime* sebagai "*crime related to technologi,computer, and the internet*" atau secara sederhana berarti kejahatan yang berhubungan dengan teknologi, komputer dan internet.[29]

Dalam beberapa literatur, *cyber crime* sering di identikkan sebagai *computer crime*. Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" mengartikan *cyber crime* sebagai kejahatan di bidang computer. secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Menurut freddy haris, *cyber crime* merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

1. *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan),
2. *Unauthorized alteration or destruction of data*,
3. Menggangu/merusak operasi komputer,
4. Mencegah/menghambat akses pada komputer.[30]

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.

Barda Nawawi Arief, *Cyber Crime menurut Convention on Cyber Crime* 2001 di Budapest Hongaria adalah sebagai berikut.

---

[29] *Ibid.*halaman 13
[30] Didik M. Arief Mansyur, Elisatris Gultom, Opcit, halaman 9

1. *Illegal access* yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.
2. *Illegal interception* yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis.
3. *Data interference* yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.
4. *System interference* yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer
5. *Misuse of Devices* yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk *(access code).*
6. *Computer related Forgery* yaitu pemalsuan dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik.
7. *Computer related Fraud* yaitu penipuan dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data computer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan

untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain.[31]

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. Berdasarkan jenis aktifitas yang dilakukannya, *cyber crim*e dapat digolongkan menjadi beberapa jenis:

Hacking adalah kegiatan menerobos program komputer milik orang/pihak lain. *Hacker* adalah orang yang gemar eksplorasi komputer, memiliki keahlian membuat dan membaca program tertentu, dan terobsesi mengamati keamanan (*security*). "*Hacker*" memiliki 2 wajah ganda: "*WHITE HAT HACKER"* memberi tahu kepada admin yang komputernya diterobos, bahwa adanya kelemahan-kelemahan pada program yang dimiliki dan punya potensi disusup. Karakteristik *White Hat Hacker* ini adalah memberikan informasi bukan merusak yang pasti menguntungkan/membantu korbannya. *"BLACK HAT HACKER*", menerobos program orang lain untuk merusak, manipulasi/merubah serta mencuri datanya. Karakteristik *Black Hat Hacker* ini adalah melakukan aktifitas kriminal yang pasti merugikan korbannya.

Cracking adalah *hacking* untuk tujuan jahat. Sebutan pelaku *cracking* adalah *"cracker"* Aktfitas *Cracker* sejenis dengan "*hacker* bertopi hitam" (*BLACK HAT*

[31] Remy Syahdeini, Sutan. 2011. *Kejahatan & Tindak Pidana Komputer*. Jakarta : PT Pustaka Utama Grafiti. halaman 93.

HACKER). Berbeda dengan "*carder*" yang hanya mengintip kartu kredit, *"cracker*" mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, "*hacker*" lebih fokus pada prosesnya. Sedangkan "*cracker"* lebih fokus untuk menikmati hasilnya.

Carding adalah Aktifitas berbelanja secara *online* tertapi menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, pelaku *carding* biasa disebut *carder.* Sebanyak 20 persen transaksi melalui internet yang berasal dari Indonesia adalah hasil *carding*. Akibatnya, banyak situs belanja online yang memblokir *IP address* (alamat komputer internet) yang berasal dari Indonesia. Menurut *ICT Watch*, Lembaga Swadaya Masyarakat yang mengamati dunia internet di Indonesia, para *carder* sekarang beroperasi semakin jauh, *carder* juga melakukan penipuan melalui forum-forum di milis dan ruang chatting di *mIRC.*

Defacing adalah kegiatan mengubah halaman situs pihak lain, seperti yang terjadi pada situs Presiden SBY, Kemenkominfo dan Partai Golkar, BI dan situs KPU saat pemilu 2004 lalu. Banyaknya kasus *deface* saat ini yang bermotif iseng belaka mereka ingin unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga pelaku *deface* yang jahat, mereka melakukan aktifitas *deface* untuk mencuri data dan dijual kepada pihak lain.

Fishing atau Phising adalah kegiatan memancing pengguna internet dengan harapan agar *user* secara tidak sadar memberikan informasi data *user* dan *password* nya pada *website* yang sudah dilakukan *deface.*

Spamming adalah pengiriman berita atau iklan lewat surat elektronik *(e-mail)* yang tak dikehendaki. *Spam* sering disebut juga sebagai *bulk email* atau *junk email* alias "sampah". Meski demikian, banyak juga orang yang terkena dan menjadi korbannya.[32]

[32] Garda T. Paripurna. 2008 . *Sekilas Tentang Kejahatan Transnasional* . Riset Hukum Kejahatan Transnasional

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Kebijakan Hukum Pidana Dalam Penanggulangan *Cyber Crime* di Indonesia .

1. Kasus *cyber crime* di indonesia

a. *Defacing*

Situs milik KPU (Komisi Pemilihan Umum) *Defacing* oleh *hacker*. Peristiwa tersebut terjadi pada tanggal 17 April 2004 dengan target situs http://tnp.kpu.go.id. Tampilan lambang 24 partai diganti dengan nama partai lucu 'partai jambu', 'partai cucak rowo', 'Partai Kolor Ijo' dan lainnya. Pelakunya, diketahui, bernama Dani Firmansyah 24 tahun mahasiswa asal Yogyakarta yang kemudian ditangkap Polda Metro Jaya. Motivasi pelaku, hanya ingin menjajal sistem pengamanan di *server* KPU yang dibeli sangat mahal dan anti bobol katanya saat itu. Tapi ternyata berhasil di tembus oleh Dani. Ketiadaan undang-undang *cyber* di Indonesia membuat Dani Firmansyah dijerat dengan pasal-pasal Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengancam pidana terhadap perbuatan: "memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan eletromagnetik terhadap penyelenggaraan telekomunikasi".

Dani Firmansyah, juga dijerat melakukan tindak pidana yang melanggar pasal 22 huruf a, b, c, Pasal 38 dan Pasal 50 Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi. Pada pasal 22 UU Telekomunikasi berbunyi:

Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jaringan telekomunikasi dan atau akses ke jasa telekomunikasi; dan atau akses ke jaringan telekomunikasi khusus. Sedangkan bunyi pasal 50 UU No 36/1999 tentang Telekomunikasi berbunyi "Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)."

b. *Phising*

Kasus klik bca merupakan kasus *domain name* yang memanfaatkan kesalahan ketik yang bisa dilakukan oleh para nasabahnya. Steven Haryanto membeli 5 domain plesetan pada situs target www.klikbca.com yakni www.klikbca.com, kilkbca.com, clikbca.com, klickbca.com dan klikbca.com. Target dari Steven Haryanto adalah nasabah BCA yang melakukan salah ketik dalam penulisan klikbca, tampilan *homepage web* plesetan sama persis dengan *homepage* BCA. *User* akan melakukan login disitus-situs *phising* tersebut, *user name* dan *PIN* internet korban akan terkirim pada sang pemilik situs. Steven Haryanto yang sudah meminta maaf dan menyerahkan semua *user ID* dan *PIN* kepada BCA. Kasus tsb tidak dilanjutkan ke pengadilan karena Steven memberikan informasi security BCA yang masih lemah. Saat itu pihak BCA tengah memikirkan alternatif lain ketimbang melaporkan Steven ke polisi. Steven Haryanto merupakan contoh karakteristik "*WHITE HAT HACKER"*.

c. Pornografi,

Larangan melakukan perbuatan yang bermuatan melanggar kesusilaan diatur dalam Pasal 27 ayat (1) dan diancam sanksi pidana berdasarkan Pasal 45 ayat (1). Pasal 27 ayat (1) menentukan: 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. Ancaman pidana terhadap pelaku yang melanggar Pasal 27 ayat (1) ditentukan dalam Pasal 45 ayat (1) yang berbunyi: Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (5), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000.00 (satu miliar rupiah).

Awal Juni 2010 publik dikejutkan dengan munculnya tiga buah video mesum tiga artis ibu kota, yaitu Nazriel Irham (Ariel), Luna Maya dan Cut tari. Dalam pengakuannya Ariel mengatakan bahwa ia merasa kecolongan atas file pribadi yang diperuntukkan untuk dikonsumsi secara pribadi. Namun, hukum pun harus berjalan. Ariel dijerat pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi dan Elektronik yang berbunyi: ’’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”. Ariel juga di jerat Pasal 29 UU Pornografi: Setiap orang yang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor,

mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi sebagaimana dimaksud. Majelis Hakim Pengadilan Negeri Bandung menjatuhkan hukuman 3,5 tahun penjara kepada Ariel dalam kasus video asusila tersebut.

Actus reus, adalah "*conduct"* atau perilaku yang dapat berupa melakukan perbuatan tertentu yang dilarang oleh undang-undang atau "*commission*" atau "*act"* atau berupa berdiam diri atau tidak melakukan perbuatan yang diwajibkan oleh hukum atau "*omission*"" yaitu berdiam diri tidak berbuat sesuatu. *Actus reus* dari tindak pidana Pasal 27 ayat (1) jo. Pasal 45 ayat (1) adalah: mendistribusikan, mentransmisikan, dan/atau membuat dapat diakses *Mens rea* (sikap kalbu) atau unsur kesalahan dari tindak pidana tersebut di atas adalah "dengan sengaja". Objek dari *actus reus* tindak pidana tersebut adalah Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

d. Kasus Pencemaran Nama Baik

Larangan melakukan penghinaan dan atau pencemaran nama baik dengan menggunakan sistem komputer diatur dalam Pasal 27 ayat (3) dan diancam sanksi pidana berdasarkan Pasal 45 ayat (1). Pasal 27 ayat (3) menentukan: 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. Ancaman pidana terhadap pelaku yang melanggar Pasal 27 ayat (3) ditentukan dalam Pasal 45 ayat (1) yang berbunyi: Setiap Orang yang memenuhi unsur

sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Prita Mulyasari merupakan seorang pasien Rumah Sakit Omni Internasional Alam Sutra Tangerang. Kasus ini terjadi saat ia dirawat di Rumah Sakit tersebut Prita tidak mendapat kesembuhan namun penyakitnya malah bertambah parah. Pihak rumah sakit tidak memberikan keterangan yang pasti mengenai penyakit Prita, dan pihak Rumah Sakit tidak memberikan rekam medis yang diperlukan oleh Prita. Kemudian Prita Mulyasari mengeluhkan pelayanan rumah sakit tersebut melalui email yang kemudian menyebar ke berbagai mailing list di dunia maya. Pihak Rumah Sakit Omni Internasional marah, dan merasa dicemarkan nama baik nya oleh Pita. Pihak RS Omni International mengadukan Prita Mulyasari secara pidana. Prita terjerat Undang-undang Nomor 11 Tahun 2008, Pasal 27 ayat (3) tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam pasal tersebut tertuliskan: "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". Pasal 27 ayat (3) ini kemudian menurut para Ahli hukum dan praktisi ICT sering disebut pasal karet, Kedua kata kunci di pasal itu adalah "dengan SENGAJA" dan "TANPA HAK".

Menurut banyak pakar. Tersangka tidak dengan Sengaja mau menghina atau mencemarkan nama baik karena ia hanya menyampaikan keluhan mengenai apa yang ia alami, Hak tersebut juga diatur dalam UU Perlindungan Konsumen."

Prita punya hak untuk menyampaikan keluhan mengenai apa yang dialaminya. Karena Prita merupakan konsumen ia adalah pasien dari rumah sakit tersebut. Adanya Kasus ini akan membawa dampak sangat buruk dan membuat masyarakat takut menyampaikan pendapat, kritik, saran atau komentarnya di dunia maya. Pasal UU ITE ini harus direvisi, setidaknya tidak boleh dipakai sebagai rujukan hukum hingga nanti terbit PP (Peraturan Pemerintah) dan Permen/Kepmen Kominfo yang menjadi turunan hukumnya.[33]

e. Peretasan Situs Negara

Membobol Komputer dan/atau Sistem Elektronik yang bertujuan selain untuk mengakses juga untuk menaklukkan sistem pengamanan dari sistem komputer yang diakses itu. Larangan melakukan perbuatan tersebut diatur dalam Pasal 30 ayat (3) yang berbunyi: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Melanggar larangan Pasal 30 ayat (3) dipidana berdasarkan Pasal 46 ayat (3) yang berbunyi: Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah). Actus reus dari tindak pidana tersebut di atas adalah "mengakses". Mens rea dari tindak pidana tersebut di atas adalah "dengan sengaja".

[33]Rudi Hermawan, " *Kesiapan aparatur pemerintah dalam menghadapi cyber crime di Indonesia*". Jurnal Media Hukum . Vol. 6 No. 1 , 25 september 2019, halaman 11.

Objek dari *actus reus* tindak pidana tersebut adalah sama saja dengan objek dari actus reus dalam Pasal 30 ayat (l) dan ayat (2), yaitu "Komputer dan/atau Sistem Elektronik". Namun yang berbeda adalah tujuan pelakunya.

Peretasan Situs Negara www.presidensby.info, Pada 9 Januari 2013 situs www.presidensby.info di retas. Saat diretas, Halaman depan diganti dengan latar belakang hitam dengan tulisan warna hijau di bagian atas "*Hacked by MJL007*", sementara di bawahnya tertera sebuah logo dan tulisan "Jemberhacker Team" berwarna putih. Wildan ditangkap setelah melakukan *deface* situs SBY www.presidensby.info Wildan Yani S (22 th) peretas situs SBY lulusan SMK tahun 2010, Wildan memang tidak melanjutkan kuliah karena terhambat biaya. Wildan bekerja sebagai operator warung Internet di Jember. Wildan ditangkap pada 25 Januari lalu, terancam dengan melanggar Pasal 50 jo. Pasal 22 huruf b Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Wildan terancam hukuman pidana penjara paling lama 6 tahun penjara dan atau denda paling banyak Rp 600 juta. Wildan juga dinilai melanggar Pasal 46 Ayat (1), (2), dan (3) jo. Pasal 30 Ayat (1), (2), dan (3) serta Pasal 48 Ayat (1) juncto Pasal 32 Ayat (1) UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Serangkaian pasal itu mengancam Wildan dengan hukuman penjara 6 hingga 10 tahun serta denda mencapai Rp 5 miliar.

Namun, Kepolisian menganggap motif Wildan hanya iseng mengganti tampilan situs tersebut tanpa ada maksud politik. Bareskrim Polri mendata, Wildan akan direkrut sebagai staf *cyber crime* Mabes Polri. Tetapi Kepolisian tetap memproses kasus Wildan. Saat ini sedang tahap penyelesaian perkara.

Penangkapan Wildan ini kemudian memicu reaksi dari kelompok *hacker* internasional terkemuka, *ANONYMOUS*. Mereka meminta wildan di bebaskan dari segala tuntutan karena aksi wildan tidak merusak sistem maupun datanya tapi bersifat memberitahu dan mengingatkan bahwa pengelolaan situs penting milik pemerintah belum maksimal menjaga keamanannya, bila tuntutannya tidak dipenuhi mereka menyatakan "perang" terhadap situs Pemerintah Republik Indonesia dengan menumbangkan situs-situs berdomain "go.id". Situs-situs yang sudah dilumpuhkan antara lain beberapa sub domain di situs KPPU, BPS, KBRI Tashkent,Kemenkumham, Depsos, dan Kemenparekraf, bahkan Indonesia.go.id.[34]

2. Kebijakan *cyber crime* melalui pendekatan KUHP

Hukum Pidana yaitu bagian dari keseluruhan hukum yang berlaku disuatu Negara, yang mengadakan dasar-dasar dan peraturan untuk menentukan perbuatan perbuatan yang tidak boleh dilakukan, menentukan kapan dan hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenakan atau dijatuhi pidana sebagaimana yang telah diancamkan, menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar tersebut.

Tindak Pidana dapat juga dikatakan dengan perbuatan pidana yang memiliki definisi sebagai berikut : “Perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa melanggar larangan tersebut”.

[34]Arifiyadi Teguh . 2008 . *Menjerat Pelaku Cyber Crime dengan KUHP*. Pusat Data Departemen Komunikasi dan Informatika diakses pada tanggal 27 september 2019 dari www. depkominfo.go.id

Saat ini, Indonesia sudah memiliki Undang Undang *cyber law* yang mengatur mengenai *cyber crime* .Rancangan undang undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari rancangan undang-undang tindak pidana di bidang teknologi informasi sejak tahun 2016 sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki.

Kitab Undang-Undang Hukum Pidana (KUHP) merupakan hukum nasional adalah sumber hukum sekaligus payung hukum untuk menindak berbagai macam tindak pidana yang terjadi di Indonesia. Dalam kaitannya dengan masalah *cyber crime,* KUHP nasional pengaturannya dapat digolongkan menjadi dua, yaitu pengaturan secara umum/tidak langsung dan pengaturan secara khusus/ langsung. Pengaturan secara langsung artinya mengatur secara eksplisit tindak pidana yang berhubungan dengan kejahatan *cyber crime*.

Kebijakan kriminalisasi Cyber Crime (CC) dalam Rancangan Undang-Undang Pemanfaatan Teknologi Informasi (RUU-PTI) tertuang dalam Bab XIV yang berjudul "Ketentuan Pidana" mulai Pasal 35-40. Undang-Undang Pemanfaatan Teknologi Informasi (RUU-PTI) pada intinya memuat perumusan tindak pidana seperti apa yang terdapat dalam Konvensi *Cyber Crime* Dewan Eropa (*Council of Europe Cyber Crime Convention*) 2001 yaitu:[35]

[35]Barda Nawawi Arief, 2012 . *Kapita Selekta Hukum Pidana*, Bandung: PT. Citra Aditya Bakti, , halaman 256-258.

Pasal 35:

- Memuat Perumusan delik mengenai "penggunaan nama domain yang bertentangan dengan Hak Kekayaan Intelektual milik orang lain";
- Dalam Konvensi *Cyber Crime*, delik serupa ini termasuk "*infringement of copyright"*.

Pasal 36:

- Memuat perumusan delik mengenai "mengaksis data komputer/media elektronik lainnya secara melawan hukum";
- Dalam Konvensi *Cyber Crime*, delik ini disebut dengan istilah "*illegal access"*.

Pasal 37:

- Ayat (1) memuat perumusan delik mengenai perbuatan "menahan atau mengintersepsi pengiriman data melalui komputer/media elektronik lainnya secara melawan hukum"; dan ayat (2)-nya memuat perumusan delik mengenai perbuatan. "mengintersepsi secara melawan hukum pengiriman data melalui komputer/media elektronik yang menghambat komunikasi dalam sistem komputer/jaringan komputer/sistem komunikasi lainnya";
- Dalam Konvensi *Cyber Crime*, delik dalam Pasal 37 di atas, disebut "*illegal interception*" untuk ayat (1) dan termasuk "*interference system*" untuk ayat (2)

Pasal 38:

- Ayat (1) memuat perumusan delik mengenai perbuatan ‘memasukkan, mengubah, menambah, menghapus atau merusak data komputer/program komputer/data elektronik lainnya secara melawan hukum”. Delik pada ayat (1) itu diperberat ancaman pidananya apabila “mengakibatkan kerugian ekonomi bagi orang lain” ayat (2) dan “mengakibatkan terganggunya fungsi sistem komputer atau sistem media elektronik lainnya ayat (3);
- Dalam Konvensi *Cyber Crime*, delik dalam ayat (1) dan ayat (2) tergolong “*data interference*” dan ayat (3) termasuk “*system interference*”.

Pasal 39:

- Memuat perumusan delik mengenai penggunaan kartu kredit/alat pembayaran elektronik lainnya milik orang lain secara melawan hukum dalam transaksi elektronik.
- Delik ini dalam Konvensi *Cyber Crime* termasuk “*computer related offences”*, khususnya “*computer related fraud*”.

Pasal 40:

- Ayat (1) memuat ketentuan mengenai perbuatan “membuat, menyediakan, mengirimkan, mendistribusikan, data/tulisan/gambar/rekaman yang isinya melanggar kesusilaan dengan menggunakan komputer/media elektronik lainnya”. Delik pada ayat (1) diperberat ancaman pidananya dalam ayat (2) apabila objeknya adalah anak.

- Dalam Konvensi *Cyber Crime*, hanya disebutkan adanya "*child pornography*" seperti pada ayat (2) di atas.

Tindak pidana di atas Pasal 35-40 diancam dengan pidana penjara (maksimumnya berkisar antara 1 (satu) sampai dengan 5 (lima) tahun dan/atau pidana denda (maksimumnya berkisar antara Rp. 100.000.000,00 (seratus juta rupiah) sampai dengan Rp. 500.000.000,00 (lima ratus juta rupiah).

Dalam Upaya Menangani kasus kasus yg terjadi khususnya yang ada kaitannya dengan *cyber crime*, para Penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP Pasal yang dapat dikenakan dalam KUHP pada *cyber crime* antara lain:

a. KUHP (Kitab Undang-Undang Hukum Pidana), pasal-pasal yang terkait :
    1. Pasal 362 KUHP tentang pencurian (Kasus *carding*) *Carding* sendiri dalam versi Polri meliputi:
        a) Mendapatkan nomor kartu kredit dari tamu hotel, khususnya orang asing;
        b) Mendapatkan nomor kartu kredit melalui kegiatan *chatting* di Internet;
        c) Melakukan pemesanan barang ke perusahaan di luar negeri dengan menggunakan Jasa Internet;
        d) Mengambil dan memanipulasi data di Internet;
        e) Memberikan keterangan palsu, baik pada waktu pemesanan maupun pada saat pengambilan barang di Jasa Pengiriman;

f) *Carding* (pelakunya biasa disebut *carder*), adalah kegiatan melakukan transaksi *e-commerce* dengan nomor kartu kredit palsu atau curian. Pelaku tidak harus melakukan pencurian atau pemalsuan kartu kredit secara fisik, melainkan pelaku cukup mengetahui nomor kartu dan tanggal kadaluarsanya saja;

g) Pasal 378 KUHP tentang Penipuan (Penipuan melalui *website* seolah-olah menjual barang);

h) Pasal 311 KUHP Pencemaran nama Baik (melalui media internet dengan mengirim email kepada Korban maupun teman-teman korban);

i) Pasal 303 KUHP Perjudian (permainan judi online);

j) Pasal 282 KUHP *Pornografi* (Penyebaran *pornografi* melalui media internet).

2. Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Khususnya tentang Program Komputer atau software
3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomukasi, (penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi).
4. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang-Undang No.15 Tahun 2002 tentang Pencucian Uang.
5. Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme.

Beberapa langkah penting yang harus dilakukan dalam penanggulangan *cyber crime* adalah :

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber crime*
d. Meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya mencegah kejahatan tersebut terjadi
e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaties*.

3. Kebijakan *cyber crime* melalui pendekatan UU ITE

Kejahatan merupakan entitas yang selalu melekat dengan dinamika perkembagan peradaban umat manusia. Kejahatan yang oleh Saparinah Sadli disebut sebagai perilaku menyimpang, selalu ada dan melekat pada setiap bentuk masyarakat; tidak ada masyarakat sepi dari kejahatan.

Oleh karena itu, upaya penanggulangan kejahatan sesungguhnya merupakan usaha yang terus menerus dan terus berkesinambungan. Semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu

pengetahuan dan teknologi,muncul berbagai jenis kejahatan berdimensi baru, yang termasuk di dalamnya *cyber crime*. Sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi ketertiban masyarakat.

Akan tetapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab terhadap dampak negatif yang timbul dari kejahatan. Hal ini dikarenakan teknologi yang membawa perubahan dalam masyarakat berkembang begitu pesat, sementara hukum pidana merupakan produk sejarah tertentu berjalan dengan logika sejarah yang menaunginya walaupun dalam batas tertentu mempuntyai prediktabilitas atas perkembangan masyarakat.

Dua muatan besar yang diatur dalam UU ITE ialah mengenai pengaturan tranksaksi elekronik dan mengenai tindak pidana siber. Materi UU ITE tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional. Pada UU ITE dimuat tentang perbuatan yang dilarang pada Pasal 27 sampai Pasal 36. Pada pasal 42 UU ITE diatur pula mengenai ketentuan penyidikan yang berbunyi : "penyidikan sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam undang

undang ini".

Dengan demikian, sistem pembuktian yang dianut adalah sistem/teori pembuktian berdasar undang-undang secara negatif, yaitu sistem yang dianut dalam KUHAP dan berdasar Pasal 183 KUHAP, yang berbunyi sebagai berikut: "hakim tidak boleh menjatuhkan pidana kepada sesorang kecuali apabila dengan

sekurang-kurangnya dua alat bukti yangsah ia memperoleh keyakinan bajwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya". Dengan demikian, artinya pembuktian harus didasarkan ketentuan undang-undang, yakni alat bukti yang sah yang diatur dalam Pasal 184 KUHAP disertai keyakinan hakim yang diperoleh dari alat-alat bukti tersebut. Berikut beberapa alat bukti yang diatur dalam Pasal 184 KUHAP sebagai acuan dalam pembuktian kejahatan mayantara (*cyber crime*), yaitu:

a. Keterangan saksi Syarat formal keterangan saksi yang diatur dalam KUHAP ialah, antara lain, dinyatakan di persidangan dan mengucapkan sumpah atau janji sebelum saksi memberikan keterangan. Sedangkan syarat materiil untuk keterangan saksi antara lain:
    1) Keterangan yang diberikan ialah mengenai peristiwa yang ia dengar, lihat, dan alami sendiri dengan menyebutkan alasan pengetahuannya.
    2) Bukan pendapat, rekaan, maupun keterangan ahli
    3) Ada lebih dari satu orang saksi yang sesuai asas *unus testis nullus testis*;bukan keterangan yang dia peroleh dari orang lain (*testimonium de auditu);*
    4) Adanya persesuaian antara keterangan saksi yang satu dengan yang lain dan keterangan saksi yang satu dengan alat bukti yang lain.
    5) Pada kasus *cyber crime*, dikarenakan sifatnya yang *virtual*, maka pembuktian dengan menggunakan keterangan saksi tidak dapat diperoleh secara langsung. Keterangan saksi hanya dapat berupa hasil pembicaraan atau hanya mendengar orang lain. Kesaksian ini dikenal

dengan *testimonium de auditum atau hearsay evidence*, meskipun kesaksian sejenis ini tidak diperkenakan sebagai alat bukti, akan tetapi dalam praktiknya tetap dapat dipergunakan sebagai bahan pertimbangan bagi hakim untuk memperkuat keyakinannya sebelum menjatuhkan putusan. Kemungkinan yang dapat dijadikan keterangan saksi ialah melalui hasil interaksi dalam dunia *cyber*, seperti *chatting* dan *e-mail* antara pengguna internet, atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi.

b. Keterangan ahli Dalam Pasal 186 KUHAP diatur mengenai syarat formil keterangan ahli bahwa keterangan ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Yang disebut sebagai ahli ialah ahli kedokteran kehakiman dan ahli lainnya. Keterangan ahli menjadi signifikan penggunaannya jika jaksa mengajukan alat bukti elektronik untuk membuktikan kesalahan pelaku *cyber crime*. Peran keterangan ahli disini adalah untuk memberikan suatu penjelasan dalam persidangan bahwa dokumen/data elektronik yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum.

c. Alat bukti surat (Pasal 184 huruf c dan Pasal 187 KUHAP)

   Jenis surat yang diakui berdasarkan alat bukti ialah surat yang dibuat diatas sumpah jabatan atau dikuatkan dengan sumpah sebagaimana yang tertuang dalam pasal 187 KUHAP. "Surat" dalam kasus *cyber crime* mengalami perubahan dari bentuknya yang tertulis menjadi tidak tertulis

dan bersifat *online.* Alat bukti dalam komputer yang telah disertifikasi ada dua kategori. Pertama, bila sebuah sistem komputer yang telah disertifikasi oleh badan yang berwenang, maka hasil print out komputer dapat dipercaya keotentikannya. Contohnya *receipt* yang dikeluarkan oleh suatu bank dalam transaksi ATM. Alat bukti ini mempunyai kekuatan pembuktian meskipun dalam persidangan dibutuhkan keterangan lebih lanjut. Kedua, bukti sertifikasi dari badan yang berwenang tersebut dapat dikategorikan sebagai bukti surat, karena dibuat oleh dan atau pejabat yang berwenang. Jenis alat bukti surat lainnya dapat berupa bukti elektronik yang dapat dicetak dan surat yang terpampang dalam layar monitor sebuah jaringan komputer. Selama kedua bukti ini dikeluarkan/dibuat oleh yang berwenang dalam sebuah sistem jaringan komputer dan sebuah sistem jaringan komputer tersebut dapat dipercaya, maka surat tersebut memiliki kekuatan pembuktian yang sama dengan alat bukti surat sebagaimana yang ditentukan dalam KUHAP.

d. Alat bukti petunjuk (Pasal 184 (1) huruf d dan Pasal 188 KUHAP) KUHAP mengatur secara *limitatif* mengenai sumber petunjuk, yaitu bahwa petunnjuk hanya dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa. Untuk dapat dijadikan sumber petunjuk, ketiga alat bukti tersebut harus sah, dan oleh karena itu, petunjuk yang dihasilkan juga menjadi sah.Dalam *cyber crime,* pengumpulan alat bukti secara fisik akan sulit dipenuhi. Yang paling mudah dalam melakukan pengumpulan bukti-bukti adalah mencari petunjuk-petunjuk yang mengindikasi telah

adanya suatu niat jahat berupa akses secara tidak sah. Misalnya dengan melihat dan mendengarkan keterangan saksi di pengadilan, atau surat elektronik atau hasil *print out data*, atau juga dari keterangan terdakwa di pengadilan.

e. Keterangan terdakwa (Pasal 184 huruf e dan Pasal 189 KUHAP) Keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. Agar keterangan terdakwa dapat dinyatakan sah, syarat formil,yaitu dinyatakan di sidang dan syarat materiil keterangan tersebut tentang perbuatan yang terdakwa lakukan atau ketahui atau alami sendiri – harus dipenuhi. Dalam Undang-undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik pasal 5 ayat 1 dan 2 mendeskripsikan bahwa Dokumen Elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. Selain dalam pasal 44 Undang-undang yang sama mengatakan : "Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undang undang ini adalah sebagai berikut :

   1) alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan.
   2) alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Informasi Elektronik dan Dokumen Elektronik dapat dijadikan sebagai alat bukti yang sah menurut undang-undang tentang Teknologi Informasi dan Transaksi Elektronik, walaupun sulit untuk diklasifikasikan termasuk alat bukti yang sah sebagaimana dimaksud Pasal 184 ayat (1) KUHAP. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai ketentuan yang diatur dalam UU ITE.[36]

B. Penegakan Hukum *Cyber Crime* Di Indonesia Melaui Sarana Penal dan Non Penal.

1. Penegakan Hukum *Cyber Crime* Melalui Sarana Penal.

Sebelum penulis membahas penegakan hukum *cyber crime* dengan sara penal, penulis lebih dulu akan mengemukakan masalah intrumen internasional yang berkaitan dengan kejahatan *cyber*. Intrumen internasional yang berkaitan dengan *cyber crime* adalah *Convention on Cyber Crime* tanggal 23 November 2001 di kota Budapest Hongaria telah membuat dan menyepakati *Convention on Cyber Crime* yang kemudian dimasukkan dalam *European Treaty Series* dengan nomor 185.[37]

Convention on Cyber Crime 2001 dibentuk dengan pertimbangan antara lain:[38]Pertama, masyarakat internasional menyadari perlunya kerjasama antara negara dan industri dalam memerangi kejahatan *cyber* dan adanya kebutuhan untuk melindungi kepentingan yang sah di dalam penggunaan serta pengembangan teknologi informasi. Kedua, Konvensi saat ini diperlukan untuk

---

[36]Sehatapy, J.E. 2004 . *Pisau Analisis Kriminologi*. . Bandung. : PT Citra Aditya Bakti . halaman 113

[37] Ahmad M.Ramli . 2012 . *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia* . Bandung: PT Refika Aditama . halaman 23

[38]*Ibid*. halaman 23-24

meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Dengan demikian perlunya adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat. Ketiga, saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk perlindungan Hak Azasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekpresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi dan pendapat.

Dilihat dari kebijakan kriminal (kebijakan penanggulangan kejahatan), hukum pidana bukan merupakan sarana kebijakan yang strategis. Kebijakan yang strategis adalah mencegah dan meniadakan faktor faktor penyebab atau kondisi yang menimbulkan kejahatan. Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cyber crime*) tentunya tidak dapat dilakukan secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistemik. Sebagai salah satu bentuk dari high tech crime, merupakan hal yang wajar jika upaya penanggulangan *cyber crime* juga harus ditempuh dengan teknologi (*techno prevention*).

Disamping itu diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan global (kerjasama internasional) karena *cyber crime* dapat melampaui batas-batas negara (bersifat *transnational/*

transborder).Walaupun sarana penal mempunyai keterbatasan, namun dilihat dari sudut "perencanaan kebijakan penanggulangan kejahatan dengan hukum pidana" (*penal policy*), tahap kebijakan legislasi/formulasi merupakan tahap paling strategis. Kesalahan/kelemahan kebijakan legislatif merupakan kesalahan strategis yang dapat menjadi Penghambat upaya pencegahan dan penanggulangan kejahatan pada tahap aplikasi dan eksekusi.[39]

Dalam upaya atau kebijakan penanggulangan *cybercrime* dengan hukum pidana, lokakarya/workshop mengenai *"computer related crime*" yang diselenggarakan dalam kongres PBB X (April 2000) menyatakan, bahwa negaranegara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur. Jadi masalahnya bukan sekedar bagaimana membuat kebijakan hukum pidana (kebijakan kriminalisasi, formulasi, dan legislasi) di bidang penanggulangan *cyber crime*, tetapi bagaimana ada harmonisasi kebjakan penal di berbagai negara. Ini berarti, kebijakan kriminalisasi tentang masalah *cyber crime* bukan semata-mata masalah kebijakan nasional (Indonesia) tetapi juga terkait dengan kebijakan regional dan internasional.

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakekatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan

[39]Barda Nawawi Arif, op , cit ,.halaman 53

menggunakan sarana hukum pidana (penal), dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" (*penal policy)*, khususnya kebijakan formulasinya.

Ketentuan hukum pidana positif yang dikriminalisasi terkait kejahatan mayantara (*cyber crime*) dapat kita lihat pada Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana yang dimuat pada Pasal 27 sampai dengan Pasal 36. Terdapat pula pada Undang-undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi, dimana sisi mayantara dari tindak pidana korupsi ini adalah bahwa kejahatan tersebut telah menggunakan media internet sebagai alat untuk melakukan korupsi ataupun memperlancar tindak dilakukannya tindak pidana tersebut meskipun tidak secara eksplisit diatur dalam undang-undang ini. Beberapa peraturan perundang-undangan yang mengkriminalisasi kejahatan mayantara di dalamnya adalah : Undang-undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, dan Undang-undang Nomor 35 Tahun 2009 tentang Narkotika.

Ada beberapa peraturan perundang-undangan yang berkaitan dengan masalah komputer, di antaranya adalah sebagai berikut:

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

Suatu program atau data mempunyai nilai puluhan kali lipat dibandingkan nilai dari komputer atau media lainnya dimana data atau program tersebut

tersimpan yang menjadikan banyak orang yang ingin mengambilnya secara tidak sah untuk disalah gunakan atau diambil manfaat tanpa izin pemiliknya.[40] Menurut Pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, bahwa program komputer adalah sekumpulan intruksi yang diujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak Cipta untuk program komputer berlaku selama 50 tahun (Pasal 30). Harga program komputer/software yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual *software* bajakan dengan harga yang sangat murah. Maraknya pembajakan *software* di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan pemilik Hak Cipta. Tindakan pembajakan program komputer tersebut merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah)".

[40]Barda Nawawi Arief, op. cit., halaman 135-135

b. Undang-undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme

Undang-undang Nomor 5 Tahun 2018 mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf (b) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. *Digital evidence* atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap internet lebih sulit dibandingkan pelacakan melalui *handphone*.

Berkaitan dengan penggunaan hukum pidana, Nigel Walker sebagaimana dikutip oleh Muladi, mengatakan bahwa ada 6 (enam) syarat prinsip yang harus diperhatikan oleh pembentuk undang-undang, yaitu:

1) Hukum pidana tidak digunakan semata-mata untuk tujuan pembalasan;
2) Tindak pidana yang dilakukan harus menimbulkan kerugian dan korban yang jelas;
3) Hukum pidana tidak digunakan apabila masih ada cara lain yang lebih baik dan lebih prima;
4) Kerugian yang ditimbulkan karena pemidanaan harus lebih kecil daripada akibat tindak pidana;
5) Harus mendapat dukungan masyarakat; dan

6) Harus dapat diterapkan dengan efektif.

Perlu diperhatikan juga pendapat Sudarto mengenai penggunaan hukum pidana dan kriminalisasi suatu perbuatan menjadi tindak pidana, sebagai berikut :

1) Hukum pidana harus digunakan untuk mewujudkan masyarakat adil dan makmur,
2) merata materiil dan spiritual.
3) Hukum pidana bertugas untuk menanggulangi kejahatan dan tindakan penanggulangan itu sendiri untuk kesejahteraan masyarakat atau untuk pengayoman masyarakat.
4) Hukum pidana digunakan untuk mencegah atau menanggulangi perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian pada masyarakat.
5) Penggunaan sarana hukum pidana dengan sanksi yang negative perlu disertai dengan perhitungan biaya yang harus dikeluarkan dan hasil yang diharapkan akan dicapai (*cost and benefit principle).* [41]

2. Penegakan Hukum *Cyber Crime* Melalui Sarana Non Penal.

Pendekatan non penal menurut Hoefnagels adalah pendekatan pencegahan kejahatan tanpa menggunakan sarana pemidanaan (*prevention without punisment)*, yaitu antara lain perencanaan kesehatan mental masyarakat (*community planning mental health*), kesehatan mental masyarakat secara nasional (*national mental health*), *social worker and child welfare* (kesejahteraan anak dan pekerja sosial),

[41]Budi Agus Riswandi . 2006 . *Hukum Cyberspace* . Yogyakarta: Gitanagari

serta penggunaan hukum civil dan hukum administrasi (*administrative & civil law*).

Kebijakan penanggulangan kejahatan lewat jalur "non penal" lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan. Oleh karena itu, sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan yang berpusat pada masalah-masalah atau kondisi-kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuh suburkan kejahatan. Dengan demikian dilihat dari kebijakan penanggulangan kejahatan, maka usaha-usaha non penal ini mempunyai kedudukan yang strategis dan memegang peranan kunci yang harus diintensifkan dan diefektifkan.

Beberapa masalah dan kondisi sosial yang dapat merupakan faktor kondusif penyebab timbulnya kejahatan, jelas merupakan masalah yang tidak dapat diatasi semata–mata dengan "penal". Di sinilah keterbatasan jalur "penal" dan oleh karena itu, harus ditunjang oleh jalur "non penal". Salah satu jalur "non penal" untuk mengatasi masalah–masalah sosial seperti dikemukakan diatas adalah lewat jalur "kebijakan sosial" (*social policy*), dimana G.P. Hoefnagels juga memasukkan dalam jalur "prevention without punishment". Kebijakan sosial pada dasarnya adalah kebijakan atau upaya-upaya rasional untuk mencapai kesejahteraan masyarakat. Jadi identik dengan kebijakan atau perencanaan pembangunan nasional yang meliputi berbagai aspek yang cukup luas dari pembangunan.

Cyber Crime membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Beberapa langkah

penting yang harus dilakukan setiap negara dalam penanggulangan *cyber crime* adalah:

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber crime*
d. Meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya mencegah kejahatan tersebut terjadi.
e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime,* antara lain melalui perjanjian ekstradisi dan *mutual assistance treaty.*
f. Harmonisasi mengenai masalah yurisdiksi untuk menegakkan kedaulatan negara yang berlaku karena sifatnya transnasional.

Meskipun hukum pidana digunakan sebagai ultimum remidium atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasan tersebut dikemukakan oleh Barda nawawi Arief sebagai berikut :

a. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;
b. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;
c. Hukum pidana hanya merupakan bagian kecil (subsistem) dari sarana kontrol sosial yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemayarakatan yang sangat kompleks (sebagai masalah sosio-psikologis, sosio-politik, sosio-ekonomi, sosio-kultural dan sebagainya);
d. Penggunaan hukum pidana dalam menanggulangi kejahatan hanya merupakan "*kurierenam symptom*", oleh karena itu hukum pidana hanya merupakan pengobatan simptomatik dan bukan pengobatan kausatif;
e. Sanksi hukum pidana merupakan *remedium* yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif;
f. Sistem pemidanaan bersifat *fragmentair* dan individual/personal, tidak bersifat struktural/fungsional;
g. Keterbatasan jenis sanksi pidana dan sistem perumusan sanksi pidana yang bersifat kaku dan imperatif;
h. Bekerjanya/berfungsingnya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan memerlukan "biaya tinggi".

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh Polri yang menggunakan hukum pidana sebagai landasan kerjanya. Sebab

kejahatan yang kompleks ini terlambat diantisipasi oleh Polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya. Untuk itu, pencegahan kejahatan tidak melulu harus menggunakan hukum pidana. Agar penegakan hukum *cyber crime* ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Dari paparan penegakan hukum dengan sarana non-penal ini, maka menurut penulis cara non- penal inilah yang lebih diutamakan dari pada sarana penal dengan konsekwensi segera menyiapkan penegak hukum yang menguasai teknologi informasi. Atau lebih jelasnya kita sangat membutuhkan Polisi *cyber*, Jaksa *cyber,* Hakim *cyber* dalam rangka penegakan hukum *cyber crime* di Indonesia tanpa adanya penegak hukum yang mempuni di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat *cyber* oleh karena kejahatan *cyber* ini *locus delicti* bisa lintas negara.

C. Faktor – Faktor Yang Mempengaruhi Dalam Penanggulangan *Cyber Crime* di Indonesia

Hukum tumbuh bukan dari perbuatan pemerintah, tetapi dari fakta-fakta sosial di dalam suatu komunitas. Aturan hukum merupakan pencerminan kaidah-kaidah ekonomi dan moral yang didasarkan pada pengakuan masyarakat tentang kesignifikanannya bagi ikatan masyarakatnya. Oleh sebab itu keberadaan aturan yang mengatur mengenai prostitusi *cyber* didasarkan pada kaidah ekonomi dan moral

Secara umum kejahatan komputer dapat dicegah melalui faktor-faktor lingkungan yaitu:

1. Pendidikan komputer sejak dini yang dimulai dari bangku sekolah, sehingga dapat meningkatkan pengetahuan dan kesadaran atas bentuk-bentuk perbuatan dalam menggunakan sarana komputer yang salah.
2. Pengawasan terhadap warnet-warnet yang ada di masyarakat , untuk mencegah warnet sebagai sarang penggunaan situs yang melanggar hukum.
3. Pengawan orang tua terhadap anak pengguna komputer dan internet.
4. Membuat wadah bagi anak-anak yang memiliki kelebihan dibidang jaringan internet. Filterisasi situs-situs yang merusak norma anak muda oleh pemerintah.
5. Sanksi yang tegas bagi pemilik warnet jika tidak menegur users nya yang sedang menggunaan situs *cyber gambling, cyberporn* , dll.
6. Banyaknya komunitas *black hat* (hacker hitam) di Indonesia sebagai salah satu dampak penyebab maraknya terjadi kejahatan di dunia maya, lemahnya *system computer*, dan begitu kecilnya gaji para ahli IT di Indonesia menyebabkan para master computer berbuat criminal demi mencukupi kebutuhan *financialnya* , jadi perlu peningkata taraf hidup bagi para ahli IT.

1. Faktor penangulangan *cyber crime* melalui para penegak hukum

Strategi Penanganan Pemerintah Penyempurnaan perangkat hukum, Polri, Kemenkominfo, DPR, pakar hukum dan organisasi lainnya yang sangat

berkepentingan atau keamanan usahanya tergantung dari kesempurnaan undang-undang di bidang *cyber space* (pengusaha *e-commerce dan banking*) sedang memproses untuk merancangnya agar di Indonesia terwujud UU ITE yang sempurna. UU ITE diharapkan bersifat *lex specialist*, menyempurnakan undang undang pendukungnya dan melakukan sintesa serta analogi yang lebih luas terhadap KUHP. UU ITE yang sudah ada perlu direvisi terutama pasal / ayat yang karet (multitafsir), setidaknya tidak boleh dipakai sebagai rujukan hukum hingga nanti terbit PP dan Permen/Kepmen Kominfo yang menjadi turunan hukumnya. Perlu dilakukan Komitmen dan kerja sama yang intensif antara Kemenkominfo dengan para pakar dari universitasuniversitas dan pelaku bisnis ICT khususnya ISP dan *Computer Network Security* dalam mengantisipasi perkembangan *cyber crime* di Indonesia. Mendidik para penyidik, Dalam hal menangani kasus *cyber crime* diperlukan penyidik yang mempunyai cukup pengalaman (bukan penyidik pemula), pendidikannya diarahkan untuk menguasai teknis penyidikan dan menguasai administrasi penyidikan serta dasar-dasar pengetahuan di bidang komputer dan profil *hacker*.

Untuk itu diperlukan pengiriman aparat hukum Polisi, Jaksa, Hakim untuk melakukan pendidikan mengenai *cyber crime* di negara maju khususnya Amerika Serikat. Membangun Fasilitas *Forensic Computing*, Keberadaan *Fasilitas Forensic Computing* sangat penting dan vital dalam membongkar kasus *cyber crime.* Fasilitas *Forensic Computing* yang akan didirikan Polri diharapkan akan dapat melakukan tiga hal penting, yaitu; *Evidence Collection* (pengumpulan bukti), *Forensic Analysis* (analisis forensik), *Expert Witness* (saksi ahli).

Diharapkan nantinya Para ahli forensik komputer bisa memanfaatkan fasilitas tsb untuk mendeteksi lokasi kejahatan yang tepat dan juga mendukung dalam pemulihan dokumen yang hilang atau sengaja dirusakkan. Ahli Komputer forensik menangani dengan setiap kasus dengan sangat hati-hati ketika akan melakukan pemeriksaan forensik, Setiap melakukan kesalahan penempatan akan berakibat korupsi data atau dapat merusak sistem secara keseluruhan. Komputer forensik memungkinkan ahli forensik dapat mengetahui masing-masing dari setiap file. Baik file yang disimpan di tempat biasa dan maupun yang tersembunyi dan file yang dilindungi oleh security. Hal tersebut dapat dilakukan melalui *tool forensik. Forensik* komputer ini juga memainkan peran sebagai analisa teknis sehingga mampu menyelidiki bagian yang paling sulit terjangkau dari perangkat digital. Meningkatkan Upaya Penyidikan Dan Kerja Sama Internasional, Indonesia melalui Kepolisian RI bekerja sama dengan Amerika Serikat (AS) melalui *International Criminal Investigative Training Assistance Program (ICITAP*) melatih lebih dari 100 orang polisi se-Jawa timur mengenai cara mengatasi "*Cyber Crime"* (Tindak Kejahatan Dunia Maya). Selain itu Aparatur kepolisian melalui Kepolisian negara-negara Asean terus berkoordinasi dan bekerjasama untuk memerangi kejahatan di dunia maya atau *cyber crime.*

Untuk meningkatkan kemampuannya, sebanyak 70 perwira dari kepolisian se-Asean mengikuti pelatihan selama dua hari di Bandung. pelatihan ini juga melibatkan para ahli dari *Interpol, Apcert, Microsoft*, kepolisian Korea dan Kepolisian Federal Australia. Kerjasama Kepolisian Republik Indonesia (Polri) dengan *Australia Federal Police* (AFP), dalam bidang penanganan

kejahatan *cyber*, diharapkan mampu meningkatkan kinerja penyidik dalam menangani bukan hanya kasus *cyber crime*, namun juga terorisme di Indonesia.

2. Solusi Kebijakan Hukum Pidana Terhadap Penanggulangan *Cyber Crime* di Indonesia

Terjadinya kasus cyber crime, pihak kepolisian telah melakukan berbagai upaya penanggulangan cyber crime upaya tersebut adalah upaya preventif dan represif.

a. Upaya Preventif

Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *cyber crime* polisi telah melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik maupun media sosial dengan menyebarkan *broadcast* berupa himbauan-himbauan terkait *cyber crime* untuk di *forward* ke masyarakat luas. Selain itu dilakukan juga penerangan ke masyarakat melalui media surat kabar dan radio, serta pada saat mengisi acara *talkshow* pihak kepolisian tidak henti-hentinya memberikan himbauan kemasyarakat.

b. Upaya Represif

Pihak kepolisian bekerja sama dengan *stakeholder* yang ada yaitu bagaimana menangkap pelaku yang tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus *cyber crime*, setelah dilakukan penangkapan kemudian diproses dikepolisian dan sebelum dilimpahkan berkas perkaranya ke kejaksaan terlebih dahulu diadakan konferensi pers dengan media dimana pihak media hadir untuk

mewawancarai tersangka dan petugas yang menangani kasus tersebut. Lalu hasil wawancara tersebut disiarkan atau disebarkan kemasyarakat luas, sehingga masyarakat mengetahui kasus-kasus yang ditangani oleh aparat kepolisian

c. Pelaksanaan Undang Informasi dan Transaksi

Dalam mengahadapi *cyber crime*, hukum positif di Indonesia masih bersifat *lex locus delicti*. Namun beda halnya dengan situasi dan kondisi pelanggaran hukum yang terjadi atas *cyber crime* dimana pelaku kejahatan *cyber* dan korban berada di tempat yang berbeda. Wilayah kejahatan dunia maya yang begitu luas namun mudah diakses menyebabkan maraknya terjadi kejahatan. Kepolisian Republik Indonesia (POLRI) sebagai salah satu alat kelengkapan negara dalam menegakkan hukum tidak dapat lagi tinggal diam setelah lahirnya Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Aparat penegak hukum dalam hal ini penyidik kepolisian harus bergerak secara aktif untuk menindak kejahatan di dunia maya. Aparat kepolisian harus dapat menangani kasus-kasus kejahatan yang terjadi di dunia maya.[42]

Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) :

1) Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleteks, telecopy atau sejenisnya, huruf, tanda, angka, Kode

[42] M.Ramli, Ahmad. 2006 . *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*, Bandung: PT Refika Aditama.halaman 98.

Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

2) Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.
3) Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
4) Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
5) Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
6) Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat penyelenggara sistem elektronik adalah setiap Orang, penyelenggara

negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

7) Jaringan Sistem Elektronik adalah terhubungnya dua sistem elektronik atau lebih, yang bersifat tertutup ataupun terbuka.
8) Agen Elektronik adalah perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu informasi elektronik tertentu secara otomatis yang diselenggarakan oleh orang.
9) Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Penyelenggara sertifikasi elektronik.
10) Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.
11) Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam transaksi elektronik.
12) Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

13) Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan tanda tangan elektronik.
14) Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.
15) Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
16) Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.
17) Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.
18) Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.
19) Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.
20) Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21) Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.

22) Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.

23) Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Preside

Cyber crime di Indonesia khususnya dalam (UU ITE) dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatanperbuatan yang menjadikan komputer sebagai sasaran kejahatan. Kejahatan yang menggunakan komputer sebagai sarana adalah setiap tindakan yang mendayagunakan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukan kejahatan di ruang maya bukan ruang nyata. Kejahatan yang menjadikan komputer sebagai sasaran adalah setiap perbuatan dengan menggunakan komputer yang diarahkan pada data komputer, sistem komputer, atau jaringan komputer, atau ketiganya secara bersama-sama. Perbuatan tersebut dilakukan di ruang maya bukan ruang nyata, sehingga seluruh aktivitas yang dilarang oleh peraturan perundangundangan terjadi di ruang maya.[43]

[43]Undang – undang ITE No.19 tahun 2016

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Kebijakan Hukum Pidana melalui pendekatan KUHP untuk menangggulangi tindak pidana *cyber crime* di Indonesia masih memiliki tumpang tindih hukum dan masih belum seutuhnya terkandung didalam produk KUHP ,terjadi banyak analogi terkait penjeratan hukum terhadap tersangka *cyber crime* seperti kasus *carding* yang dikaitkan dengan pasal pencurian yakni, pasal 368 KUHP. Juga terjadi pada pendekatan UU ITE yang belum seluruhnya mengatur berbagai tindak pidana *cybercrime* itu sendiri sehingga belum memiliki payung hukum yang pasti.
2. Penegakan Hukum *cyber crime* di Indonesia secara penal, masih mengacu pada sistem Kitab Undang-Undang Hukum Acara Pidana (KUHAP) secara mutlak. Sedangkan secara non penal dilakukan melalui metode atau pendekatan sosial seperti informasi himbauan,jalur pendidikan, pembinaan, dan juga terkait hal-hal pencegahan *cyber crime* tersebut.
3. Faktor – faktor yang mempengaruhi dalam penanggulangan tindak pidana *cyber crime* di indonesia. Upaya Preventif dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *cyber crime* polisi telah melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik . Upaya Represif Pihak kepolisian bekerja sama dengan *stakeholder* yang ada yaitu bagaimana menangkap pelaku yang

tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus *cyber crime*.

B. Saran

1. Dalam mewujudkan penegakan hukum perlu peran aktif aparat penegak hukum yaitu dengan dibekali keahlian khusus dalam melakukan penyidikan dan penyelidikan guna memperlancar pembuktian kejahatan mayantara (*cyber crime*) tersebut. Peningkatan sarana prasarana dan kemampuan aparat penegak hukum di bidang teknologi dan informasi, pengetahuan, keyakinan dan pandangan yang luas hakim dalam menafsirkan hukum sebagai upaya penegakan hukum dunia mayantara di Indonesia.
2. Dalam mewujudkan penegakan hukum perlu peran aktif aparat penegak hukum yaitu dengan dibekali keahlian khusus dalam melakukan penyidikan dan penyelidikan guna memperlancar pembuktian kejahatan mayantara (*cyber crime*) tersebut. Peningkatan sarana prasarana dan kemampuan aparat penegak hukum di bidang teknologi dan informasi, pengetahuan, keyakinan dan pandangan yang luas hakim dalam menafsirkan hukum sebagai upaya penegakan hukum dunia mayantara di Indonesia. Dan perlu peningkatan kelengkapan alat teknologi informasi dan komunikasi untuk memperlancar proses pembuktian kejahatan

tersebut serta peningkatan kerjasama internasional dalam rangka penegakan hukum untuk memberantas kejahatan mayantara (*cyber crime).*

3. Terkait faktor penanggulangan *cyber crime* sejauh ini cukup memuaskan, namun diperlukan sosialisasi atau seminar dari pihak Kepolisian yang bekerja sama dengan perwakilan pemerintah melalui Menkominfo terkait *cyber crime* dan juga unsur serta klasifikasi terkait tindak pidana tersebut.

DAFTAR PUSTAKA

A. Buku

Abdul Manan. 2013. *Aspek –Aspek Pengubah Hukum*. Jakarta: Kencana.

Abdul wahid dan Mohammad Labib. 2015. *Kejahatan Mayantara (Cyber Crime).* Jakarta: PT Refika Aditama.

Arifiyadi Teguh. 2008. *Menjerat Pelaku Cyber Crime dengan KUHP*. Pusat Data Departemen Komunikasi dan Informatika.

Barda Nawawi Arief. 2016. *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*. Jakarta: Prena Media Group.

Budi Suhariyanto. 2012. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: RajaGrafindo Persada.

Didik M. Arief Mansyur, (dkk). 2015. *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Reflika Aditama.

Elaw dan Pewit. 2016. *Kebijakan Publik*. Jakarta: Pustaka Prima.

Garda T. Paripurna. 2008. *Sekilas Tentang Kejahatan Transnasional*. Riset Hukum Kejahatan Transnasional.

Ida Hanifah, (dkk). 2018. *Pedoman Penulisan Tugas Akhir Mahasiswa*. Medan: UMSU Pers.

M. Ramli, Ahmad. 2006. *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*. Bandung: PT Refika Aditama.

Prasetyo, Teguh, dan Barkatullah, Abdul Halim. 2011. *Politik Hukum Pidana Kajian Kebijakan Kriminalisasi dan Dekriminalisasi.* Yogyakarta: Pustaka Pelajar.

Rahardi, H. Pudi, Hukum Kepolisian . 2014. *Kemandirian, Profesionalisme Dan Reformasi Polri*. Surabaya: Laks Bang Grafika.

Remy Syahdeini, Sutan. 2011. *Kejahatan & Tindak Pidana Komputer*. Jakarta : PT Pustaka Utama Grafiti.

Rukmini. 2014. *Aspek Hukum Pidana dan Kriminologi (Sebuah Bunga Rampai).* Bandung: P.T. Alumni.

Sehatapy, J.E. 2004. *Pisau Analisis Kriminologi*. Bandung: PT Citra Aditya Bakti.

Soerjono Soekanto. 2013. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: PT. RajaGrafindo Persada.

Sudarto. 2012. *Hukum dan Hukum Pidana*. Jakarta: Rajawali Pers.

Suparni, Neniek . 2012 . *Cyber Space Problematika & Antisipasi Pengaturannya*. Jakarta: Sinar Grafika.

Widodo . 2013. "*Sistem Pemidanaan dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime",* Yogyakarta: Laksbang Mediatama

B. Artikel, Majalah dan Jurnal Ilmiah

Ach Tahir, *"Penegakan Hukum Cyber Crime di Indonesia".* Vol. 3 No. 1

Dista Amaliah Arifah, "*Kasus Cyber Crime Di Indonesia*". Jurnal Bisnis dan Ekonomi. Vol. 18 No. 2, September 2011.

Hardianto Djanggih, " *Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan*". Jurnal Media Hukum. Vol. 1 No. 2, September 2013.

Ineu Rahmawati, *"Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense"*. Jurnal Pertahanan dan Bela Negara. Vol 7 No. 2

Rudi Hermawan, "*Kesiapan aparatur pemerintah dalam menghadapi cyber crime di Indonesia*". Jurnal Media Hukum. Vol. 6 No. 1 , 25 September 2019.

C. Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik selanjutnya disebut Undang-Undang ITE

Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme

Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jalan Kapten Muchtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website : http://www.umsuac.id, http://www.fahum.umsu.ac.id E-mail : rektor@umsu.ac.id, fahum@umsu.ac.id

UMSU
Unggul | Cerdas | Terpercaya

Bila menjawab surat ini, agar disebutkan nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

KARTU BIMBINGAN SKRIPSI MAHASISWA

NAMA : **MUHAMMAD MUIS**
NPM : **1506200471**
PRODI/BAGIAN : **ILMU HUKUM/HUKUM PIDANA**
JUDUL SKRIPSI : **KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN *CYBER CRIME* DI INDONESIA**
Pembimbing : **Dr. T. Erwinsyahbana, S.H., M.Hum**

TANGGAL	MATERI BIMBINGAN	TANDA TANGAN
14/08-2019	Skripsi diterima	
22/08-2019	Perbaikan Judul dan rumusan masalah	
31/08-2019	Penambahan materi rumusan masalah ketiga	
06/09-2019	Perbaikan Footnote dan penulisan sub judul	
14/09-2019	Koreksi materi Rumusan masalah pertama	
20/09-2019	Koreksi materi dan penulisan rumusan kedua	
26/09-2019	Koreksi materi rumusan ketiga dan BAB IV	
02/10-2019	Perbaikan Kesimpulan, saran, dan Acc	

Diketahui,
DEKAN FAKULTAS HUKUM

(Dr. Ida Hanifah, S.H., M.H)

DOSEN PEMBIMBING

(Dr. T. Erwinsyahbana, S.H., M.Hum)