BAB I

PENDAHULUAN

A. Latar Belakang

Penggunaan sistem dan alat elektronik telah menciptakan suatu cara pandang baru dalam menyikapi perkembangan teknologi. Perubahan paradigma dari *paper based* menjadi *electronic based*. Dalam perkembangannya, *electronic based* semakin diakui keefisienannya, baik dalam hal pembuatan, pengolahan, maupun dalam bentuk penyimpanannya.[1]

Perkembangan yang pesat dari teknologi telekomunikasi dan teknologi komputer menghasilkan internet yang multifungsi, perkembangan ini membawa kita keambang revolusi ke empat dalam sejarah pemikiran manusia bila di tinjau dari kontruksi pengetahuan umat manusia yang dicirikan dengan cara berfikir yang tanpa batas (*borderless way of thinking*).

Internet merupakan simbol material Embrio masyarakat global. Internet membuat globe dunia, seolah-olah menjadi seperti hanya selebar daun kelor. Era reformasi ditandai dengan eksabilitas informasi yang amat tinggi. Dalam era ini, informasi merupakan komoditi utama yang diperjualbelikan sehingga akan muncul berbagai *network* dan *information company* yang akan memperjualbelikan fasilitas bermacam jaringan dan berbagai basis data informasi tentang berbagai hal yang dapat diakses oleh pengguna dan pelanggan.

[1] Edmon Makarim, *Pengantar Hukum Telematika*, cet.I, PT. Raja Grafindo Persada: Jakarta, 2005, hlm. 447.

Internet menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi dibalik itu, timbul persoalan berupa kejahatan yang dinamakan *cybercrime*, baik sistem jaringan komputernya itu sendiri yang menjadi sasaran maupun komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. Tentunya jika kita melihat bahwa informasi itu sendiri telah menjadi komoditi maka upaya untuk melindungi asset tersebut sangat diperlukan. Salah satunya dengan melalui hukum pidana, baik dengan bersarana penal maupun non penal.

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dari dunia internasional. Vollodymyr Golubev menyebutnya sebagai *the new form of anti-social behavior*. Kehawatiran terhadap ancaman (*threat*) *cybercrime* yang telah terungkap dalam makalah *Cybercrime* yang disampaikan dalam ITAC (*information Technology Association of Canada*) pada *International Information Industry Congress (IIC) 2000 Milenium Congres di* Quebec pada tanggal 19 September 2000, yang menyatakan bahwa *cybercrime is a real growing threat to economic and social development aspect of human life and so can electronically enabled crime*[2].

Kejahatan ini merupakan tindak kejahatan melalui jaringan sistem komputer dan sistem komunikasi baik lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual dengan melibatkan pengguna internet sebagai korbannya. Kejahatan tersebut seperti misalnya manipulasi data (*the trojan horse*), spionase, *hacking*, penipuan kartu keredit online (*carding)*,

[2] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*, PT Raja Grafindo Persada: Jakarta, 2006, hlm. 2.

merusak sistem (*cracking*), dan berbagai macam lainnya. Pelaku *cybercrime* ini memiliki latar belakang kemampuan yang tinggi di bidangnya sehingga sulit untuk melacak dan memberantasnya secara tuntas.

Dewasa ini kita dapat melihat bahwa hampir seluruh kegiatan manusia mengandalkan teknologi yang menghadirkan kemudahan bagi penggunanya berupa akses bebas yang dapat dilakukan oleh siapapun, kapanpun dan dimanapun tanpa sensor serta ditunjang dengan berbagai penawaran internet murah dari penyedia jasa layanan internet. Kemudahan yang ditawarkan oleh aktivitas siber itu sendiri contohnya ketika melakukan jual-beli barang atau jasa tidak memerlukan lagi waktu yang lama untuk bertemu langsung dengan penjual atau pembelinya, sehingga waktu yang digunakan lebih cepat.

Indonesia telah menggeser kedudukan Ukraina sebagai pemegang presentasi tertinggi terhadap *cybercrime.* Data tersebut berasal dari penelitian Verisgin, perusahaan yang memberikan pelayanan intelejen di dunia maya yang berpusat di California, Amerika Serikat. Hal ini juga ditegaskan oleh Staf Ahli Kapolri Brigjen Anton Tabah bahwa jumlah *cybercrime* di Indonesia adalah yang tertinggi di dunia. Indikasinya dapat dilihat dari banyaknya kasus pemalsuan kartu kredit, penipuan perbankan, judi *online,* terorisme, dan lain-lainnya.[3]

Memanfaatkan teknologi dalam kehidupan sehari-hari telah menjadi gaya hidup masyarakat kita, akan tetapi penggunaan teknoligi tersebut tidak didukung dengan pengetahuan untuk menggunakannya dengan baik. Hasil Lembaga Riset Telematika Sharing Vision menempatkan Tahun 2013 Indonesia menjadi negara

[3] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*, Rajawali Pers: Jakarta, 2013, hlm. 17.

urutan pertama target kejahatan dunia maya. Hasil riset itu menyebutkan selama Tahun 2013 ada 42 ribu serangan *cyber* saban harinya. Dimitri Mahayana dalam seminar '*Indonesia Cyber Crime Summit* 2014' di ITB menyebutkan bahwa saat ini masyarakat Indonesia menduduki peringkat pertama dunia dengan persentase sebesar 23,54 persen sebagai pengguna internet terbesar.[4]

Setiap terjadi kejahatan maka dapat dipastikan akan menimbulkan kerugian pada korbannya. Korban kejahatan menanggung kerugian karena kejahatan, baik materiil maupun immateriil. Korban kejahatan yang pada dasarnya merupakan pihak yang paling menderita dalam suatu tindak pidana, tidak memperoleh perlindungan sebanyak yang diberikan oleh undang-undang kepada pelaku kejahatan. Akibatnya, pada saat pelaku kejahatan telah dijatuhi sanksi pidana oleh pengadilan, kondisi korban kejahatan tidak dipedulikan.[5] Kerugian baik materiil maupun immateriil yang ditimbulkan bernilai sangat besar dan dalam waktu yang relatif singkat bila dibandingkan dengan kejahatan konvensional yang lebih mudah dilokalisir. Sehingga diperlukan upaya penanggulangan bagi kejahatan teknologi informasi ini baik upaya pencegahan kejahatan secara preventif maupun penanggulangan kejahatan secara represif.

Kehadiran hukum pidana sangat diperlukan agar dapat mengatasi *cybercrime* yang semakin berkembang. Upaya penanggulangan tersebut sewajarnya menjadi jaminan bagi pengguna internet agar dapat melakukan

[4]http://www.merdeka.com/peristiwa/hasil-riset-hukum-tahun-2013-Indonesia-target-utama-kejahatan-cyber.httml, diakses pada 15 Maret 2017.

[5] Dikdik M. Arief Mansur & Eliksatris Gultom, *Urgensi Perlindungan Korban Kejahatan,* PT. Raja Grafindo Persada: Jakarta, 2007, hlm. 24

aktivitas *cyber* dengan nyaman dan aman serta diharapkan kepada seluruh masyarakat dapat turut aktif.

Menurut Mochtar Kusumaatmadja[6], hukum mempunyai kekuasaan untuk melindungi dan mengayomi seluruh lapisan masyarakat sehingga tujuan hukum dapat tercapai dalam mewujudkan keadilan sosial bagi seluruh rakyat Indonesia dan sekaligus berfungsi sebagai sarana penunjang perkembangan pembangunan secara menyeluruh.

Teknologi informasi seharusnya memberikan manfaat dan kesejahteraan untuk menunjang aktivitas sehari-hari, maka dengan konsepsi tersebut pemanfaatan teknologi informasi harus berdasarkan pada asas-asas yang dimuat dalam Pasal 3 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya disingkat dengan (UU ITE) yaitu:

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Selanjutnya pada Pasal 15 menyatakan :

(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Illegal Content merupakan salah satu bentuk pengelompokan kejahatan yang berhubungan dengan teknologi informasi (TI). *Illegal Content* dapat di

[6] Budi Suhariyanto, *Op.Cit*, hlm. 99

definisikan sebagai kejahatan dengan memasukan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Dalam artian sederhana, adalah merupakan kegiatan menyebarkan seperti mengunggah dan menulis hal yang salah atau dilarang yang dapat merugikan orang lain.[7]

Pentingnya pengaturan *illegal content* dalam UU ITE didasarkan setidaknya pada dua hal. Pertama, perlunya perlindungan hukum seperti perlindungan yang diberikan dalam dunia nyata atau fisik (*real space*). Dunia siber merupakan dunia virtual yang diciptakan melalui pengembangan teknologi informasi dan komunikasi.

Pada dasarnya konten merupakan informasi yang dapat mempengaruhi perilaku seseorang. Pornografi dan judi dapat menimbulkan kecanduan, pembuatan informasi elektronik khususnya pornografi dapat atau bahkan sering melanggar hak asasi manusia. Selain itu penyebaran konten dapat membentuk opini publik. Rusaknya kehormatan atau nama baik seseorang akibat opini publik yang terbentuk melalui penyerangan terhadap kehormatan atau nama baik orang tersebut merupakan alasan diaturnya ketentuan penghinaan dalam *cyberspace*. Kerusuhan antar suku, agama, ras, dan golongan (SARA) juga dapat terjadi akibat penyebarluasan informasi sensitive tentang SARA.

Kedua, dengan adanya internet, informasi dapat disebar dan diteruskan ke berbagai penjuru dunia dengan seketika serta dapat diakses dari berbagai Negara.

[7] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*, PT Raja Grafindo Persada: Jakarta, 2006, hlm. 42.

Terlebih lagi setiap orang dapat menggunakan nama lain selain nama diri yang sebenarnya di *cyberspace* baik secara anonym atau dengan nama samaran.

Yang dimaksud dalam *illegal content* menurut undang-undang ini adalah informasi atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan, atau pencemaran nama baik, dan pemerasan atau pengancaman sebagai mana termuat dalam pasal 27 UU ITE.

Dalam Pasal 27 Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menyatakan:

1. Setiap orang "dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan"
2. Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memiliki muatan perjudian.
3. Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memiliki muatan Penghinaan / Pencemaran Nama Baik.
4. Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memiliki muatan pemerasan atau pengancaman.[8]

Akhir-akhir ini sering terjadi penyebaran hal-hal yang tidak teruji kebenaran akan faktanya yang tersebar bebas di internet, baik itu dalam bentuk foto, video maupun berita-berita. Dalam hal ini tentu saja mendatangkan kerugian bagi pihak yang menjadi korban dalam pemberitaan yang tidak benar tersebut, seperti kita ketahui pasti pemberitaan yang beredar merupakan berita yang sifatnya negatif.

[8] Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Dalam beberapa tahun terakhir ini marak terjadi pemberitaan yang tidak benar *(Hoax)* diantaranya yang menimpa walikota Bandung Ridwan Kamil. Sang walikota Bandung pun segera merespon tindakan tersebut melalui akun media sosial. Dan segera melaporkan kepada pihak yang berwajib.

Sebelumnya Wali Kota Bandung Ridwan Kamil mengakui kesal mendapat serangan secara terbuka dan kasar di media sosial. Tulisan akun itu dinilainya sudah menyerang pribadinya. Ridwan membantah sedang mencari sensasi atau terlalu reaktif. Pria yang akrab disapa kang Emil ini mengaku sudah biasa dicaci maki. Selain berisi nada hinaan, akun tersebut juga mengundang ancaman.[9]

Dari kasus tersebut dapat disimpulkan jika kasus penghinaan terhadap orang lain merupakan salah satu jenis *cybercrime* yang dapat dikategorikan kedalam *illegal content*. Perbuatan dalam kasus ini terdapat dalam Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

Pasal 27 ayat (3) yang berbunyi "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Eletronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik."

Ketentuan pidana dalam kasus ini terdapat dalam Pasal 45 ayat (3) yang berbunyi "Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Eletronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3), dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 750.000.000,00 (tujuh ratus lima puluh juta rupiah)."

[9]https://news.detik.com/berita-jawa-barat/d-3452789/dituduh-syiah-di-medsos-ridwan-kamil-laporkan-pemilik-akun

Yang menarik dari proses hukum dalam tindak pidana "*Illegal Content*" ini ialah hanya pelaku penyebaran, pengunggahan, atau penghinaan di media sosial saja yang mendapat sanksi pidana kemudian dianggap selesai. sedangkan tidak ada perhatian khusus terhadap korban, sehingga korban muncul sebagai orang yang dilupakan serta sebagai individu yang dirugikan.

Permasalahan tersebut yang mendorong penulis untuk meneliti dan mengkaji tindak pidana *cyber illegal content*, melalui penyusunan skripsi dengan judul "**TINJAUAN *VIKTIMOLOGIS* TERHADAP KORBAN TINDAK PIDANA *CYBERCRIME ILLEGAL CONTENT* DI WILAYAH HUKUM POLRESTABES BANDUNG DIHUBUNGKAN DENGAN UNDANG-UNDANG NO 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NO 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK".**

B. Rumusan Masalah

Berdasarkan latar belakang masalah di atas dapat dirumuskan kedalam beberapa rumusan masalah sebagai bahan kajian guna menganalisis masalah yang ada dan menemukan sebuah solusi atas masalah tersebut, diantaranya:

1. Bagaimanakah kedudukan korban dalam tindak pidana *cybercrime illegal content* di wilayah hukum Polrestabes Bandung?
2. Bagaimanakah perlindungan hukum terhadap korban tindak pidana *cybercrime illegal content* menurut Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik?

3. Upaya apakah yang dilakukan oleh Polrestabes Bandung dalam menanggulangi adanya korban tindak pidana *cybercrime illegal content* di kota Bandung?

C. Tujuan Penelitian

Adanya tujuan penelitian adalah sebagai jawaban atas rumusan masalah yang dihasilkan sehingga dapat diketahui maksud dari dibuatnya penelitian terhadap masalah yang menjadi pembahasan ini, adapun tujuannya antara lain:

1. Untuk mengetahui kedudukan korban dalam tindak pidana *cybercrime illegal content* di wilayah hukum Polrestabes Bandung.
2. Untuk mengetahui perlindungan hukum terhadap korban tindak pidana *cybercrime illegal content* menurut Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.
3. Untuk mengetahui upaya yang dilakukan oleh Polrestabes Bandung dalam menanggulangi adanya korban tindak pidana *cybercrime illegal content* di kota Bandung.

D. Kegunaan Penelitian

1. Secara teoritis, umumnya diharapkan hasil dari penelitian ini dapat mengembangkan ilmu pengetahuan di bidang hukum, khususnya menjadi acuan bagi penulis untuk mengembangkan hasil dari penelitian ini.
2. Secara praktis, umumnya diharapkan dapat menjadikan solusi aparat penegak hukum khususnya untuk menindak lanjuti persoalan tindak pidana *cyber*

illegal content baik dalam upaya pencegahan (preventif) maupun penanggulangan (represif).

E. Kerangka Pemikiran

Tujuan dari penerapan hukum adalah untuk menjamin kehidupan dan kemaslahatan manusia serta menegakan keadilan dan kepastian hukum. Seperti halnya jika terjadi kejahatan terhadap hukum yang berlaku, harus diproses sesuai ketentuan hukum. Dalam mencegah suatu kejahatan maka harus dilakukan upaya-upaya penanggulangan baik secara preventif maupun represif.

Seiring perkembangan teknologi informatika yang semakin canggih di era globalisasi, telah membawa pengaruh terhadap munculnya berbagai jenis kejahatan yang sifatnya modern dan berdampak lebih besar dari kejahatan konvensional. Kejahatan di bidang teknologi informasi dapat digolongkan sebagai *white collar crime*[10] karena pelaku *cybercrime* adalah orang yang menguasai penggunaan internet beserta aplikasinya, sehingga menjadi ancaman bagi masyarakat, bangsa dan negara, serta merupakan tindakan yang bertentangan dengan harkat dan martabat dan dapat dikatakan sebagai suatu tindak pidana sehingga harus diberantas.

Oleh karena itu, *cybercrime* atau kejahatan dunia maya dapat dikatakan sebagai suatu kejahatan, karena *cybercrime* merupakan perbuatan yang dilarang oleh suatu aturan hukum, yaitu UU ITE.

[10] Barda Nawawi, *Op.Cit,* hlm. 1

Kata *cyber* sendiri berasal dari kata *cybermatics,* merupakan suatu bidang ilmu pengetahuan tentang mengatur atau mengarahkan sistem mulai dari yang sederhana hingga yang paling kompleks dengan cara memahami sistem melalui alat, cara dan metode.[11]

Cybercrime saat ini digunakan untuk menunjukkan kepada kejahatan yang berhubungan dengan *cyberspace* dan tindakan kejahatan yang menggunakan komputer (*computer crime). Cyberspace*[12] merupakan ruang virtual yangterbentuk dari hasil penyatuan antara manusia dan teknologi. Perkembangan *cyberspace* yang pesat menyebabkan terjadinya penyalahgunaan teknologi tersebut oleh pihak-pihak yang tidak bertanggung jawab. Penyalahgunaan yang terjadi dalam *cyberspace* inilah yang kemudian dikenal dengan *cybercrime* atau dalam berbagai literatur lain digunakan istilah *computer crime* dan sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi kejahatan komputer.

Dalam berbagai kepustakaan, *cybercrime* sering diidentikan sebagai *computer crime.* Menurut the U.S. Department of Justice "*Any illegal act requiring knowledge of Computer technology for its perpetration, investigation, or prosecution*". Pendapat lain dikemukakan oleh *Organization for Economic Cooperation Development* (OECD) yang menggunakan istilah *computer related crime* yang berarti: "*any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the tranmission of data."*[13]

[11] Josua Sitompul, *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Tatanusa: Jakarta, 2012, hlm. 4.

[12] *Ibid*, hlm. 15.

[13] Widyopramono Hadi Widjojo, "*Cybercrime dan Pencegahannya",* jurnal Hukum Teknologi, Fakultas Hukum Universitas Indonesia, hlm. 7 dalam Maskun, 2013, *Kejahatan Siber Cybercrime Suatu Pengantar",* Kencana: Jakarta, 2005, hlm. 47.

Dari berbagai pengertian *computer crime* di atas, maka dapat dirumuskan bahwa *computer crime* merupakan perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.[14]

Menurut Nazura Abdul Manaf, perbedaan mendasar antara *cybercrime* dan *computer crime* adalah adanya unsur komputer yang terkoneksi melalui perangkat telekomunikasi dalam bentuk *internet online* yang menjadi media bagi seseorang atau kelompok untuk melakukan pelanggaran dan/atau kejahatan.[15]

Berdasarkan beberapa literatur serta praktiknya, *cybercrime* memiliki beberapa karakteristik, yaitu:[16]

1. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah *cybercrime/cyberspace*, sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan menggunakan perbuatan apapun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, uang, jasa, barang, hargadiri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut dilakukan secara transansional/melintasi batas negara.

[14] *Ibid*, hlm. 48.
[15] *Ibid.*
[16] Budi Suhariyanto, *Op. Cit*, hlm. 13-14.

Sedangkan diliteratur lainnya mengelompokan *cybercrime* menjadi beberapa bentuk, antara lain:[17]

1. *Unauthorized Access to Computer System and Service*.

   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatusistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.

2. *Data Forgery*

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

3. *Cyber Espionage*.

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

[17] *Ibid,* hlm. 14

jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen.

4. Cyber Sabotage and Extortion.

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

5. Offense against Intellectual Property

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

6. *Infringements of Privacy*.

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

7. *Illegal Contents*.

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

Pelaku yang menyebarkan informasi elektronik dan/atau dokumen elektronik yang bermuatan *illegal content* dapat perseorangan atau badan hukum, sesuai isi Pasal 1 angka 21 UU ITE bahwa "Orang adalah orang perseorangan, baik warga negara Indonesia, warga Negara asing, maupun badan hukum". Keberadaan Badan Hukum diperjelas kembali dalam Pasal 52 ayat (4) UU ITE bahwa Korporasi yang melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai Pasal 37 UU ITE, termasuk menyebarkan informasi elektronik dan/atau dokumen elektronik yang bermuatan *illegal content* dikenakan pemberatan pidana pokok ditambah dua pertiga.

Perbuatan penyebaran informasi elektronik dan/atau dokumen elektronik seperti dalam Pasal 27 sampai Pasal 29 harus memenuhi unsur:

Illegal Content seperti penghinaan, pencemaran nama baik, pelanggaran kesusilaan, berita bohong, perjudian, pemerasan, pengancaman, menimbulkan rasa kebencian atau permusuhan individu, ancaman kekerasan atau menakut-nakuti secara pribadi

Dengan sengaja dan tanpa hak, yakni dimaksudkan bahwa pelaku mengetahui dan menghendaki secara sadar tindakannya itu dilakukan tanpa hak.

Pelaku secara sadar mengetahui dan menghendaki bahwa perbuatan "mendistribusikan" dan/atau "mentransmisikan" dan/atau "membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik" adalah memiliki muatan melanggar kesusilaan. Dan tindakannya tersebut dilakukannya tidak *legitimate interest*.

Perbuatan pelaku berkaitan *illegal content* dapat dikategorikan sebagai berikut:

a. Penyebaran informasi elektronik yang bermuatan *illegal content*.
b. Membuat dapat diakses informasi elektronik yang bermuatan *illegal content*.
c. Memfasilitasi perbuatan penyebaran informasi elektronik, membuat dapat diaksesnya informasi elektronik yang bermuatan *illegal content* (berkaitan dengan pasal 34 UU ITE).

F. Langkah-langkah Penelitian

Mengetahui dan membahas suatu permasalahan maka sangatlah diperlukan adanya pendekatan dengan menggunakan metode tertentu yang bersifat ilmiah. Metode yang digunakan penulis dalam penelitian ini adalah sebagai berikut:

1. Metode Penelitian

Skripsi ini termasuk penelitian dengan metode deskriptif analitis, yang menurut pendapat Komarudin, deskriptif analisis ialah:

> "Menggambarkan masalah yang kemudian menganalisa permasalahan yang ada melalui data-data yang telah dikumpulkan kemudian diolah serta

disusun dengan berlandaskan pada teori-teori dan konsep-konsep yang dipergunakan".[18]

2. Metode Pendekatan

Pada penelitian ini penulis menggunakan metode pendekatan *yuridis normatif*, penelitian hukum yang menggunakan teori/konsep dan asas-asas hukum. Rony Hanitijo berpendapat:

> "Pendekatan *yuridis normatif*, yaitu penelitian di bidang hukum yang dikonsepsikan terhadap asas-asas, norma-norma dogma-dogma atau kaidah hukum yang merupakan patokan bertingkah laku".[19]

3. Tahap Penelitian

Penelitian dalam skripsi ini dilakukan dalam 2 (dua) tahapan, yaitu:

a. Penelitian Kepustakaan (*Library Research)*

Menurut Ronny Hanitjo Soemitro, adalah:

> "Yang dimaksud dengan penelitian kepustakaan yaitu penelitian terhadap data sekunder, data sekunder dibidang hukum dipandang dari sudut kekuatan mengikatnya dapat dibedakan menjadi 3 (tiga) yaitu: bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier".[20]

(1) Bahan-bahan hukum primer yaitu, bahan-bahan yang meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-undang No 19 Tahun 2016 tentang perubahan atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Kitab Undang-Undang Hukum Pidana (KUHP), dan Hukum tidak tertulis.

[18] Martin Steinmann dan Gerald Willen dalam Komarudin, *Metode Penulisan Skripsi dan Tesis,* Angkasa: Bandung, 1974, hlm 97.

[19] Soerjono Soekanto, *Pengantar Penelitian Hukum,* UI Press: Jakarta, 1996, hlm 250

[20] Ronny Hanitjo Soemitro, *Metode Penelitian Hukum Dan Jurimentri*, Ghalia: Jakarta, 1990, hlm 11

(2) Bahan hukum sekunder ialah yang memberikan penjelasan mengenai bahan hukum primer.

Misalnya: tulisan para ahli dibidang hukum dalam bentuk karya ilmiah serta literature dan hasil penelitian yang berkaitan dengan kejahatan cyber khususnya *illegal content* dan *cybercrime*, *cyberspace*, serta *cyberlaw* khususnya UU ITE.

(3) Bahan tersier ialah bahan-bahan hukum yang memberikan petunjuk maupun penjelasan terhadap badan hukum primer dan bahan hukum sekunder.

Misalnya: bibliografi, ensiklopedia hukum dan kamus hukum.

b. Penelitian Lapangan (*Field Research)*

Tahapan ini dilakukan dalam rangka mendapatkan data primer sebagai penunjang data sekunder. Data primer diperoleh langsung melalui penelitian.[21]

4. Teknik Pengumpulan Data

Data penelitian yang ada dikumpulkan oleh penulis dengan tekhnik sebagai berikut:

a. Studi Kepustakaan (*Library Research*), yaitu melakukan penelitian terhadap dokumen yang erat kaitannya dengan hukum acara pidana dan permasalahan terhadap tindak pidana *cyber illegal content* serta penegakan hukumnya di Indonesia guna memperoleh landasan teoritis dan memperoleh informasi dalam bentuk ketentuan formal dan data melalui naskah yang resmi.

[21] Ronny Hanitijo Soemitro, *op.cit*, hlm 5

b. Studi Lapangan (*Field Research)*, yaitu memperoleh data primer dengan cara penulis mengadakan penelitian langsung untuk mendapatkan fakta yang berhubungan dengan objek penelitian di Wilayah Hukum Polrestabes Bandung.

5. Alat Pengumpulan Data

Alat pengumpulan data yang digunakan adalah, dilakukan dengan cara:

a. Pengumpulan Data

Yakni penelitian yang dilakukan dengan cara mencari dan menyimpulkan data baik literatur, wawancara, maupun perundang-undangan yang berkaitan dengan permasalahan yang diteliti. Penelitian terhadap data sekunder yang terdiri dari bahan hukum primer dan hukum tersier.

b. Pengolahan Data

Melalui data diperoleh dan dikumpulkan dari literatur atau buku, hasil wawancara dan keterangan-keterangan yang berkaitan dengan *Cybercrime, illegal content* dan hukum acara pidana, lalu dilakukan pengolahan data untuk penulisan skripsi ini.

6. Analisis Data

Metode analisis dalam penulisan skripsi ini dengan menggunakan analisis *yuridis kualitatif* yaitu data yang diperoleh dan disusun secara kualitatif untuk mencapai kejelasan masalah yang dibahas dengan tidak menggunakan rumus, kemudian data primer dan data sekunder yang diperoleh dari penelitian disusun dengan teratur dan sistematis, yang akan dinamis untuk ditarik kesimpulan.

7. Lokasi Penelitian

Penelitian ini dilakukan di wilayah hukum Polrestabes Bandung. Adapun studi pustaka dilakukan di perpustakaan UIN Sunan Gunung Djati Bandung dan perpustakaan dareah Bandung, alasan penulis dalam memilih lokasi penelitian di karenakan tindak pidana *cybercrime illegal content* merupakan hal yang menjadi masalah akhir-akhir ini yang belum secara *eksplisit* diperhatikan oleh pemerintah kota Bandung serta kurang efektivnya penegakan hukum yang dilakukan Polrestabes Bandung. Hal inilah yang mejadi ketertarikan penulis untuk melakukan penelitian di lokasi tersebut.