BAB I

PENDAHULUAN

1.1 Latar Belakang Permasalahan

Perkembangan teknologi informasi (*Information Technology*) yang pesat ini telah mengubah cara hidup manusia. Manusia mempergunakan teknologi bukan hanya untuk membuat hidup mereka lebih nyaman, tetapi juga menggantungkan sebagian aktivitas hidup mereka pada teknologi. Di sisi lain, teknologi seolah berlomba dengan para pelaku kejahatan yang memanfaatkan kecanggihan teknologi itu sendiri untuk menciptakan berbagai macam tindak kejahatan.

Keadaan ini terjadi karena dalam perkembangannya teknologi informasi berhasil menghilangkan batas-batas wilayah negara dalam melakukan aktivitas perdagangan internasional. Hilangnya batas-batas wilayah negara itu berganti dengan terhubungnya antar jaringan yang satu dengan jaringan yang lain, yang mempermudah para pelaku kejahatan dalam memperluas jangkauan tindak kejahatan yang para pelaku kejahatan lakukan yang membuat para pelaku tindak pidana *cybercrime* terus semakin kreatif menciptakan modus-modus kejahatan baru.

Di sisi lain, cepatnya perkembangan teknologi di dunia juga membuat tidak meratanya standard teknologi di tiap negara, sehingga beberapa negara secara teknologi lebih kuat dari yang lain. Tentu saja ini juga menjadi *loophole/*kelemahan tersendiri dan kelemahan-kelemahan itu dimanfaatkan

oleh para pelaku kejahatan baik dalam skala lokal maupun internasional. Kejahatan-kejahatan berbasis teknologi internet ini disebut *cybercrime*.

Definisi *cybercrime* secara umum dapat diartikan sebagai pelanggaran hukum yang memanfaatkan teknologi komputer berbasis penggunaan teknologi informasi. Sutarman mengatakan, *cybercrime* biasanya dilakukan oleh seseorang maupun sekelompok orang yang melakukan kejahatannya dengan menggunakan sarana komputer dan alat komunikasi lainya, dengan cara memasuki sistem milik orang lain tanpa ijin secara illegal atau merusak data, mencuri data, dan menggunakannya juga secara ilegal.[1]

Cybercrime disebut sebagai bentuk tindak pidana kejahatan kejahatan yang timbul karena pemanfaatan teknologi internet. Sebagai komparasi, Forester dan Morrison**,** pakar komputer asal Amerika Serikat menggambarkan bahwa kejahatan komputer merupakan suatu tindak kriminal di mana alat/senjata yang dipakai untuk melakukan tindak pidana kejahatan tersebut adalah komputer.[2] Sementara itu seorang pakar digital forensik lain, Eoghan Casey mengatakan bahwa *cybercrime* adalah suatu terminologi yang dipakai untuk mendeskripsikan aktivitas kejahatan yang mempergunakan komputer atau jaringan/jejaring komputer sebagai alat/senjata sasaran kejahatan tersebut atau sebagai tempat terjadinya kejahatan.[3]

---

[1] Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya*, (Laksbang Presindo, 2007), h.10

[2] Forester, Tom and Morrison, Perry , *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, (Boston: MIT Press, 1994), h. 5.

[3] Eoghan Casey,*Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition*,(Cambridge: Academic Press, 2011), h. 17.

Secara umum, pengertian mengenai *cybercrime* yang dapat diterima oleh hampir seluruh negara di dunia adalah *"*tindak pidana yang dilakukan dengan pemanfaatan teknologi komputer atau teknologi informasi*"*. Itulah sebabnya kerap kali para ahli menyebut *cyber crime* sebagai *computer crime.* Alat dari tindak kejahatan atau media yang dipakai untuk melakukan kejahatan itu adalah komputer. Beberapa opini lain juga mengatkan bahwa *cybercrime* adalah identik dengan *computer crime.*

Cybercrime dapat juga didefinisikan sebagai:

> *"Offences that are committed against the individuals or the groups of people with criminal motives which intentionally harm the reputation of the target /the victim or cause physical or mental harm, or loss, to the target / the victim directly or indirectly, by using modern telecommunication networks such as internet networks including chatrooms, emails, notice boards and social media groups or mobile phones (Bluetooth/SMS/MMS)".*[4]
>
> Terjemahan bebasnya adalah:
> "Setiap bentuk serangan atau tindakan yang ditujukan kepada perorangan atau kelompok dengan motif criminal/kejahatan yang dengan sengaja mengancam reputasi korban baik secara fisik maupun mental atau yang menyebabkan kerugian bagi korban langsung atau tidak langsung dan kejahatan itu dilakukan dengan menggunakan sistem jaringan telekomunikasi baik internet maupun *mobile telephone".*

Definisi itu kemudian diperluas oleh Departemen Kehakiman Amerika Serikat dengan mendefinisikan *computer crime* sebagai: "*Any illegal acts which is requiring knowledge of computer technology or informatioan technology/system for its perpetration, investigation, or prosecution".*[5] Terjemahannya adalah: Setiap tindakan melawan hukum yang memerlukan

[4] Eoghan Casey, *Digital Evidence and Computer Crime*, (Cambridge: Academic Press, 2011), h. 98.
[5] *Ibid.*,h. 121.

pengetahuan teknologi komputer untuk melakukan kejahatannya dan memerlukan juga teknologi komputer untuk menyelidiki dan menggugatnya secara hukum.

Tindak pidana *Cybercrime* yang mempergunakan teknologi berbasis utama komputer dan jaringan telekomunikasi ini pada dasarnya berdasarkan jenis aktivitas yang dilakukannya ini dapat digolongkan dalam beberapa macam seperti pada uraian berikut ini:[6]

1. *Unauthorized access* yakni; memasuki secara paksa atau menerobos kedalam suatu sistem jaringan computer diaggap melakukan kejatahatan kejahatan ini; misal *probing* dan *port;*
2. *Illegal content*; kejahatan yang dengan sengaja memasukkan informasi tentang suatu hal yang melanggar, yang tidak etis, melanggar kesusilaan atau yang buruk yang tidak benar seperti misalnya hoax atau konten pornografi yang dianggap mengganggu ketertiban umum. Contoh: Penyebaran virus secara sengaja; pada umumnya dilakukan dengan menggunakan email.
3. Data *forgery*; suatu tindak kejahatan yang dijalankan untuk memalsukan data pada dokumen-dokumen penting penting milik lembaga, institusi, perusahaan yang ada di internet. Biasanya yang penyimpanan datanya berbasis web.

[6] Besar, "Kejahatan dengan menggunakan Sarana Teknologi Informasi", https://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi ((diakses pada 21 Juni 2020, pukul 13.55).

4. *Cyber espionage, sabotage, and extortion*; Pelaku c*yber espionage* ini melakukan kegiatan mata-mata terhadap pihak lawan dengan cara memanfaatkan fungsi internet. Biasanya pelaku kejahatan jenis ini memasuki sistem komputer si target/korban dan menerobos tanpa ijin target/korban.
5. *Sabotage and extortion* adalah pengambilalihan atau penguasaan sebuah sistem yang dilakukan dengan sengaja dengan cara melakukan pengrusakan dan penghancuran terhadap data dan sistem, sehingga terjadi gangguan terhadap program komputer atau jaringan komputer yang terkoneksi dengan internet.
6. *Cyber stalking*; biasanya kejahatan jenis ini dilakukan untuk megirimkan teror/*bully*/pelecehan/gangguan terhadap seseorang dengan pemanfaatan komputer; misalnya pengiriman e-mail yang dilakukan berulang-ulang. Hal itu bisa terjadi karena sangat mudah untuk membuat email tanpa harus memberikan identitas diri.
7. *Carding;* adalah jenis ejahatan yang biasanya dilakukan seseorang dengan mencuri nomor kartu kredit milik orang lain lalu dengan nomor curian itu si pelaku melakukan transaksi di internet.
8. *Hacking* dan c*racking*; adalah 2 tindak kejahatan yang berbeda. Pelakunya disebut *Hacker* dan *Cracker*; *Hacker* adalah seseorang yang memasuki sistem targetnya untuk membongkar dan mengetahui program yang dimasuki. Pelaku *Hacking* biasanya adalah seseorang yang memiliki skill baik di bidang Teknologi informasi, kadang bahkan ahli, dengan *skill* baik

dan memiliki minat/*hobby* besar untuk mempelajari sistem komputer secara detail dalam hal meningkatkan kemampuannya.. Biasanya mereka adalah para *programmer.* Sedangkan *Cracking* dilakukan oleh seseorang yang dengan sengaja melakukan aksi-aksi pengrusakan/penerobosan sistem secara ilegal di internet. *Cracking* dimulai dengan membajak akun seseorang, situs web, probing, atau menyebarkan virus, dengan tujuan melumpuhkan target sasaran. Tindakan yang bertujuan melumpuhkan target tersebut dikenal sebagai DoS (*Denial Of Service*). *Dos attack* adalah *cyber attack* atau serangan yang ditujukan pada suatu sistem computer untuk target dan membuat sistem tersebut *crashed* atau *hanged* sehingga sistem menjadi lumpuh dan tidak dapat memberikan layanan.

9. *Cybersquatting and typosquatting;* biasanya kejahatan *cybersquatting* dilakukan dengan mendaftarkan nama domain perusahaan milik orang lain yang kemudian si pelaku kejahatan berusaha menjual kembali kepada perusahaan tersebut dengan harga yang lebih mahal. Sementara jenis kejahatan yang dilakukan dengan cara membuat domain yang mirip dengan nama domain milik orang lain disebut tuposquatting. *Biasanya domain tersebut merupakan nama domain saingan perusahaan.*
10. *Hijacking;* pada jenis kejahatan ini si pelaku kejahatan dengan sengaja membajak karya orang lain, biasanya disebut *software piracy* atau pembajakan terhadap perangkat lunak/software.
11. *Cyber terorism;* ini adalah jenis kejahatan yang ditujukan kepada pemerintah atau warganegara dengan cara melakukan *cracking* ke situs

pemerintah atau militer untuk tujuan teror. Salah satu kasus *cyber terrorism* yang cukuo terkenal adalah kasus Ramzi Yousef yang dituduh sebagai dalang serangan ke gedung WTC. Ia ditangkap karena terbukti menyimpan detail teknis file serangan dalam bentuk enkripsi di laptopnya. Kasus terkenal lain adalah kasus Doktor Nuker yang selama kurang lebih lima tahun mengelola isi situs halaman web yang berisi propaganda-propaganda anti-Amerika, anti-Israel, dan pro-Bin Laden (*defacing*).

Kejahatan dunia maya bahkan berkembang lebih luas lagi dan juga melahirkan modus kejahatan *cybercrime* yang akhirnya bahkan jauh lebih luas dan melibatkan beberapa negara yang disebut *transnational cybercrime*.[7]

Secara general kejahatan transnasional atau *transnational crime* adalah bentuk kejahatan yang dilakukan dengan melibatkan lebih dari satu negara. Artinya, tindak kejahatannya menyangkut warga negara dari dua atau lebih negara atau dilakukan di beberapa negara dan seringkali kejahatan ini mempergunakan prasarana dan sarana serta metoda-metoda yang melewati batas-batas teritorial suatu negara, melibatkan beberapa negara.

Berdasarkan hal tersebut, maka faktor utama yang menjadi identitas sebuah kejahatan transnasional adalah kejahatan-kejahatan tersebut sebenarnya terjadi di dalam satu batas wilayah negara tertentu, tetapi ada

[7] Istilah transnasional dipergunakan untuk menunjukkan kejahatan yang dilakukan oleh Individu dibebani tanggung jawab berdasarkan hukum Nasional maupun hukum Internasional. Jadi harus dibedakan dengan kejahatan Internasional yang pelakunya adalah "negara" yang dibebani tanggung jawab kriminal internasional (*international crime responsibility of state*) karena melanggar hukum Internasional. (I Wayan Parthiana, Hukum Pidana Internasional, Yrama Widya, Bandung, 2004, Hal.40)

sebagian dari unsur kejahatan tersebut berkaitan dengan negara-negara lain, misalnya tempat kejadiannya di beberapa negara, atau warga negara si pelaku kejahatan yang berasal dari beberapa negara, sehingga muncul dua atau lebih negara yang berkepentingan /terlibat atau yang terkait dengan kejahatan itu.

Faktor "melibatkan negara lain" ini lah yang membedakan jenis tindak Pidana *transnational cybercrime* dengan kejahatan pada umumnya. Pada jenis kejahatan transnasional, sifat internasionalnya bisa meliputi aspek-aspek yang apa saja yang terkait baik pelaku individu, negara yang terlibat, benda-benda terkait, publik dan privat.

Transnational cybercrime sering diartikan sebagai kejahatan dunia maya yang melibatkan lebih dari satu negara, yang dilakukan secara terorganisir, artinya dengan persiapan, perencanaan, pengarahan atau pengendalian yang dilakukan di negara lain dan berakibat bagi pihak-pihak yang dirugikan oleh negara-negara yang terlibat dalam kejahatan itu. Karena melibatkan lebih dari satu negara maka upaya penanggulangan *cybercrime* ini sering kali dalam penanganannya menemukan masalah dalam perihal yurisdiksi.

Pangkal dari pengertian yurisdiksi adalah kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum) atau kekuasaan negara. Yurisdiksi juga diartikan oleh banyak ahli sebagai suatu hak, hak atau kewenangan mutlak yang dimiliki oleh sebuah negara yang memungkinkan negara tersebut membuat peraturan-peraturan hukum, menjalankannya dan memaksakan pemberlakuannya dalam hubungannya dengan orang, benda, hal

atau masalah yang berada dan atau terjadi di wilayah suatu negara. Yurisdiksi juga merupakan bentuk refleksi dari jati diri suatu negara, prinsip dasar kedaulatan negara, bentuk persamaan derajat dari bangsa suatu negara dan serta prinsip tidak campur tangan antar negara. Yurisdiksi juga merupakan bentuk kedaulatan yang sangat penting dan krusial yang dapat menciptakan, memulai atau mengubah, serta mengakhiri suatu relasi atau kewajiban hukum.

Yurisdiksi di *cyberspace* terutama pada kejahatan transnasional, berdasar dari hukum internasional. Atas dasar prinsip-prinsip yurisdiksi dalam hukum internasional lah negara-negara di seluruh dunia dianjurkan oleh badan-badan dunia untuk berpartisipasi mengambil angkah-langkah dan pandangan yang sama dalam menjawab pertanyaan mengenai yurisdiksi internet. Hal ini disebabkan karena karakter utama *cybercrime* yang bersifat *"borderless"* atau tidak mengenal batas-batas negara sehingga dalam upaya penanggulangannya tentu memerlukan bentuk-bentuk koordinasi dan kerjasama antar negara. Permasalahan *cybercrime* dan perkembangannya menunjukkan kondisi yang kompleks dan penting dan sudah sewajarnya negara-negara di dunia mengadakan kerjasama-kerjasama internasional.

Menurut perusahaan keamanan teknologi informasi internasional *Symantec*, dalam Laporan Tahunannya *Internet Security Threat Report* volume 17, pada tahun 2011, Indonesia termasuk negara yang menempati peringkat ke 10 dengan aktivitas kejahatan *cyber* tertinggi sepanjang tahun[8].

[8]Symantec, *http://www.symantec.com/threatreport/*, *Internet Security Threat Report*, Volume 17, Indonesia, Desember 2014

Ini baru penelitian tahun 2011; pada tahun ini saja angka ini menunjukkan bahwa Indonesia menyumbang 2,4% kejahatan *cyber* di dunia. Angka ini juga menggambarkan kenaikan 1,7% dibanding tahun 2010, ketika Indonesia masih menempati peringkat ke 28.[9] Peningkatan yang sangat signifikan dan pesat ini tak lain disebabkan oleh terus meningkatnya jumlah pengguna internet di Indonesia. Pada tahun 2015, *Cybercrime* POLRI mencatat ada 800.000 akun penyebar Hoax dan 100.000 akun penyebar *"hate speech"* di Media Sosial (medsos). Riset yang dilakukan oleh jejaring sosial Facebook dan Twitter pada tahun 2016 menunjukkan bahwa Indonesia sudah masuk dalam 4 besar pengguna jejaring sosial terbanyak di dunia. Pada Tahun 2018, POLRI mengumumkan bahwa angka *cybercrime* di Indonesia adalah Nomor 2 tertinggi di Indonesia setelah Jepang. Angka kejahatan yang disebut sebagai Nomor dua di dunia itu menyangkut lebih dari 90.000.000 kasus.[10]

Kejahatan dunia maya atau *cybercrime* terus berkembang dengan cepat dan pesat sejalan dengan pesatnya perkembangan teknologi informasi itu sendiri. Kejahatan-kejahatan itu memiliki berbagai bentuk dari mulai yang paling sederhana seperti melakukan perusakan atas suatu *website* (*hacking dan cracking*), pencurian uang, *(carding*), pornografi, pemerasan, pelanggaran hak cipta, pencurian dan pembajakan data dan sebagainya. Setiap bentuk perkembangan kecanggihan teknologi informasi selalu diikuti dengan modus-modus kejahatan baru yang juga sama canggihnya.

[9] https://tekno.kompas.com/read/2012/05/16/09403718/Indonesia.Masuk.10.Besar.Penyumbang.Cyber.Crime.Terbanyak (Diakses pada tanggal 21 Juni 2020, Pukul 02.30)

[10] https://kominfo.go.id/content/detail/13487/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia/0/sorotan_media (diakses pada tnggal 21 Juni 2020, pukul 02.00)

Masalah *cybercrime* adalah masalah yang rumit dan tidak mudah untuk diselesaikan. Faktor utama kerumitannya adalah karena *cybercrime* merupakan suatu jenis kejahatan yang tidak mengenal batas wilayah hukum sehingga kejahatan tersebut dapat terjadi tanpa memerlukan interaksi langsung antara pelaku dengan korbannya. Tempat kejadian perkaranya tidak mudah untuk ditentukan. Tindakan melakukan kejahatannyapun dapat dilakukan dari belahan bumi manapun, dan korbannya juga dapat berada dimana saja.

Untuk mengantisipasi kejahatan-kejahatan *cyber*, negara-negara dengan teknologi terdepan seperti Amerika Serikat dan Inggris melakukan pengaturan yang ketat terhadap aktivitas di *cyberspace* terlebih ketika fakta-fakta di lapangan menunjukkan kegiatan *cybercrime* semakin hari semakin *sophisticated*[11]. Upaya-upaya antisipasi ini kemudian melahirkan apa yang disebut sebagai *cyber law* atau undang undang yang mengatur segala aktivitas *cyber*.

Hukum Internasional adalah instrumen hukum yang menjadi acuan Permasalahan *cybercrime* yang saat ini banyak menjadi pemikiran dunia. Rujukan negara-negara di dunia dalam hal instrument hukum internasional itu adalah konvensi tentang kejahatan dunia *cyber* (yang disebut *Convention on Cyber Crime*) 2001. Konvensi ini digagas oleh negara-negara Europa Union/Uni Eropa, sebuah rganisasi regional eropa yang menjadi penggasnya. Dalam perkembangannya konvensi ini kemudian menjadi dasar dari pemikiran

[11] *Sophisticated* adalah kata untuk menggambarkan kecanggihan suatu sistem teknologi yang memiliki makna "terdepan" dan "terunggul", *Technology Dictionary*, 2004.

penanganan masalah *cybercrime* dan bahkan banyak negara yang memiliki komitmen dalam mencegah dan menanggulangi kejahatan *cyber*, meratifikasi dan mengaksesnya. Negara-negara yang tergabung dalam Uni Eropa (*Council of Europe*) ini, pada tanggal 23 November 2001 menyelenggarakan *Convention on Cybercrime* di kota Budhapest ini.

Antisipasi *Cyber crime* adalah *Cyber law*, yang pada dasarnya merupakan bentuk hukum yang ruang lingkupnya meliputi semua aspek yang berhubungan dengan subjek hukum yang memanfaatkan dunia *cyber* dalam melakukan kegiatan apa saja baik dalam hubungannya sebagai pribadi maupun tidak.

Pengaturan atas tindakan-tindakan yang berhubungan dengan aktivitas *cyber* itu dimulai setiap kali seseorang (atau subjek hukum) memasuki dunia *cyber* dan *"on line"*. Dengan meningkatnya berbagai modus tindak pidana *cybercrime* kemudian lahirlah Undang-undang Informasi dan Tranksaksi Elektronik No. Tahun 2008 yang berisi 13 Bab dan 53 pasal yang disempurnakan dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Masalah *transnational cybercrime* adalah masalah yang sudah yang menjadi perhatian serius bagi negeri ini, terlebih dengan masuknya Indonesia dalam perdagangan global yang artinya seluruh aspek kehidupan di Indonesia, baik itu sosial, bisnis, ekonomi akan mendapatkan dampak yang signifikan dari kegiatan di dunia *cyber* ini. Publik sudah mulai terbiasa mendengar adanya

kasus-kasus kejahatan yang berhubungan dengan dunia *cyber* seperti pencurian uang *(carding*), pencurian akun jejaring sosial, penyerangan /penyebaran dengan ciptaan-ciptaan virus atau pembobolan dan perusakan *website (hacking & cracking)*, bahkan penyebaran ideologi-ideologi jahat yang merusak kerukunan masyarakat.

Pada masa-masa awal munculnya berbagai kasus yang berkaitan dengan *transnational cybercrime* di Indonesia, pihak aparat tentu saja mengalami kesulitan untuk melakukan penyelidikan dan penyidikan serta menjerat pelaku *cybercrime*. Sebagai negara yang baru saja memasuki dunia *cyber*, pengaturan yang jelas atas tindakan-tindakan yang berhubungan dengan kejahatan dunia maya tentu saja menjadi kendala yang serius, bukan saja karena kurangnya ahli-ahli komputer yang dapat membantu aparat dalam mengungkapkan sebuah kejahatan yang berbasis teknologi informasi, atau kurangnya aparat yang mememiliki pengetahuan teknologi yang mendalam, akan tetapi juga karena pada waktu itu belum ada peraturan khusus yang mengaturnya. Pada masa masa awal tersebut, tindakan-tindakan kejahatan di dunia *cyber* tidak dilihat sebagai kejahatan yang serius karena beberapa faktor yang dilihat oleh Penulis sebagai berikut:

1. Pada waktu itu (sebelum lahirnya Undang-undang ITE) sistem pembuktian di Indonesia hanya berpegang pada Pasal 184 Kitab Undang-undang Hukum Acara Pidana, yang belum mengenal istilah bukti elektronik (*digital evidence*) sebagai bukti yang sah berdasarkan undang-undang, sehingga kerap kali ketika sebuah kejahatan terjadi, namun tidak dapat diproses

sampai ke meja hijau karena dianggap tidak cukup bukti, meskipun sebenarnya ada bukti elektronik.

2. Ketiadaan peraturan yang jelas yang mengatur dunia *cyber* di Indonesia, pada waktu itu, baik itu yang mengatur mengenai masalah kewajiban-kewajiban, jaminan keamanan, jaminan kerahasiaan maupun perlindungan hukum dalam melakukan transaksi perdagangan di dunia *cyber*.

Sistem pembuktian hukum acara pidana di Indonesia yaitu *stelsel wettelijk* menekankan bahwa hanya alat-alat bukti yang sah menurut undang-undang yang dapat dipergunakan untuk memenuhi pembuktian. Pengertiannya adalah, selain dari ketentuan yang dimaksud tersebut, tidak bisa dipergunakan sebagai alat bukti yang sah.

Lahirnya *Cyber Law* Indonesia lewat Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (untuk selanjutnya disebut Undang-Undang ITE) yang disahkan pada tanggal 21 April 2008 menjadi penerangan bagi permasalahan *cyber* di negeri ini. UU ITE memang tidak sempurna, tetapi sedikit banyak menjawab tantangan kejahatan di dunia maya, akan tetapi bukan berarti masalah-masalah *cybercrime* di Indonesia sudah dapat diatasi dan ditangani dengan baik atau dengan *correct*. Undang-Undang ITE ini tentu sangat jauh dari kata sempurna. Masalah-masalah menjadi kendala dalam penyelesaian kasus-kasus-kasus *cybercrime* di Indonesia juga sama dihadapi banyak negara di seluruh dunia, yaitu pengaturan yang sama di semua negara mengenai masalah penentuan tempat kejadian perkara yaitu *Locus* dan *Tempus Delictie* dalam Penetapan Tersangka .

Undang-undang ITE telah mengakui alat bukti Digital atau bukti elektronik sebagai alat bukti yang sah di hadapan pengadilan dalam tatanan sistem hukum di Indonesia,. Kehadiran UU ITE ini pada dasarnya memperluas ketentuan Pasal 184 KUHAP mengenai alat-alat bukti yang sah dan diakui oleh Pengadilan. Untuk menentukan alat bukti yang sah dari suatu kejahatan dunia *cyber* diperlukan ahli *digital forensic*[12] yang akan bekerja berdasarkan suatu *standard operating procedure*[13] (SOP) tertentu.

Penentuan alat bukti yang sah dari suatu tindak pidana *cyber* ini akan berdampak pada penentuan mengenai tempat dan waktu kejadian perkara atau *locus delictie* dan *tempus delictie* yang penentuannya dalam banyak hal memiliki perbedaan antara *cybercrime* dengan kejahatan konvensional. Penentuan *locus & tempus delicti* tersebut dalam penetapan tersangka kasus-kasus *transnational cybercrime*, merupakan bagian dari konstruksi penetapan Tersangka dan penanganan kasus *transnational cybercrime*. Namun demikian, tidak adanya pengaturan khusus atau panduan dalam penindakan para tersangka kasus *transnational cybercrime*, membuat penanganan kasus-kasus *Transnational Cybercrime* sering kali tidak maksimal. Hal tersebut juga pernah terjadi pada beberapa kasus kejahatan penipuan dan pemerasan lintas

[12]*Digital forensic* adalah sebuah cabang dalam ilmu komputer yang mempelajari mengenai investigasi, analisa, *recovery*, dan management data dari media digital yang biasanya setelah terjadi aksi kriminal *cyber*. *Digital forensic* memiliki sub cabang keilmuan lagi, yaitu komputer forensik, *mobile device forensic, network forensic, dan database forensic*, *Technology Dictionary*, 2005.

[13]*Standard Operational Procedure (SOP)* adalah penetapan tertulis mengenai apa yang harus dilakukan, kapan, dimana, dan oleh siapa. SOP dibuat untuk menghindari terjadinya variasi dalam proses pelaksanaan kegiatan yang akan mengganggu kinerja organisasi secara keseluruhan. SOP merupakan mekanisme penggerak organisasi/lembaga agar dapat berjalan/berfungsi secara efektif dan efisien, *www.library.binus.ac.id*

negara yang dilakukan oleh segerombolan warga negara asing namun melaksanakan operasinya di Indonesia dan korbannya di Indonesia dan berbagai belahan bumi. Banyak dari kasus-kasus itu , maka terlihat bahwa penanganan terhadap para pelaku *cybercrime* transnasional hanya di proses secara administrasi keimigrasian, yaitu deportasi. Hal tersebut dikarenakan tidak adanya pengaturan yang jelas dalam penindakan tindak pidana *transnational cybercrime* di Indonesia. Polisi masih kesulitan menangani kasus-kasus tersebut dengan tuntas.

Atas dasar penjelasan di atas, maka Penulis akan mengkaji suatu penelitian yang berjudul **PENETAPAN TERSANGKA DALAM PENYIDIKAN TINDAK PIDANA *TRANSNATIONAL CYBERCRIME* MENURUT SISTEM HUKUM DI INDONESIA**

1.2. Perumusan Masalah

Berdasarkan penjabaran uraian latar belakang di atas, maka Penulis menetapkan bahwa pokok permasalahan yang akan dikaji dalam penelitian ini adalah:

1. Bagaimana penanganan penetapan tersangka dalam tindak pidana *transnational cybercrime* dalam hukum positif di Indonesia?
2. Bagaimana perbandingan penanganan tindak pidana *transnational cybercrime* di Indonesia dengan Amerika Serikat dan Inggris?

1.3. Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Untuk menganalisa konstruksi yuridis penetapan tersangka dalam tindak pidana *transnational cybercrime* dalam hukum positif di Indonesia.
2. Menganalisa penerapan di lapangan bagaimana konstruksi yuridis penetapan tersangka dalam tindak pidana *transnational cybercrime* Indonesia dan dalam dinamika perkembangan hukum pidana internasional.

1.4. Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Manfaat Teoritis

   Penulis berharap hasil penelitian tesis ini diharapkan dapat menjadi tambahan pengetahuan bagi dunia Ilmu Hukum, khususnya hukum pidana dan bagi penanganan permasalahan *transnational cybercrime* yang belakangan ini marak terjadi di dunia global dan Indonesia pada khususnya. Untuk Penulis sendiri penelitian ini memperdalam pengetahuan dalam bidang kejahatan transnasional dunia maya dan secara khusus adalah untuk memenuhi syarat kelulusan dari Program Magister Hukum UKI;

2. Manfaat Praktis

   Hasil penelitian ini diharapkan dapat memberikan masukan bagi lembaga penegak hukum dalam penyelesaian kasus yang berkaitan dengan penetapan tersangka dalam tindak pidana *transnational cybercrime*. Juga memberikan pembelajaran kepada mahasiswa hukum mengenai kejahatan *transnational cybercrime*

1.5. Kerangka Teoritis dan Kerangka Konsep

1.5.1. Kerangka Teoritis

1.5.1.1 Tujuan Pemidanaan

Hukum Pidana negeri ini adalah Kitab Undang-undang Hukum Pidana yang telah dikodifisir dari *Wetboek* yang berlaku di Indonesia Agar dapat diterapkan dengan tepat, maka Kitab Undang-undang hukum pidana tidak hanya bertujuan untuk mencari dan memberikan makna atau arti dari pasal-pasal (dogmatis) atau politis atau secara teknis perundang-undangan saja, akan tetapi juga menjadi suatu rangkaian ketentuan peraturan perundang-undangan yang memiliki makna menuju kemanfaatan bentuk logika hukum dan kepada arti kesesuaian dan atau perasaan hukum serta keadilan sebagaimana terdapat di dalam asas-asas hukum pidana yang hidup dan berlaku didalam tatanan masyarakat.

S. R. Sianturi menjelaskan dalam bukunya berjudul "Asas-asas Hukum Pidana di Indonesia" sebagai berikut: "dalam peristilahan di Indonesia, delik atau het strafbare feit diterjemahkan oleh para sarjana dan juga telah digunakan dalam berbagai perumusan undang-undang dengan berbagai istilah bahasa Indonesia sebagai perbuatan yang dapat/boleh dihukum; peristiwa pidana, perbuatan pidana atau tindak pidana.[14]

[14]Sianturi, S,R, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya*, Alumni Ahaem, Pateahaem, 1983, h.204

Sementara W.L.G Lemaire, merumuskan bahwa: "Hukum Pidana itu terdiri dari norma-norma yang berisi larangan-larangan, keharusan keharusan dan peraturan-peraturan, yang (oleh pembentuk undang-undang) dikaitkan dengan suatu rangkaian sanksi berupa hukuman, yakni bentuk-bentuk penderitaan bersifat khusus"[15] Sementara Van Hattum memberikan rumusan yang lebih kontekstual dengan realitas kehidupan sosial di Indonesia yaitu:

> "Hukum pidana disebut sebagai bentuk keseluruhan dari peraturan-peraturan dan azas-azas yang diikuti oleh suatu negara atau suatu masyarakat hukum umum lainnya, di mana mereka bertindak sebagai pemelihara dari ketertiban hukum umum yang melarang dilakukannya tindakan-tindakan yang sifatnya melanggar hukum dan pelanggaran tersebut dikaitkan dengan peraturan-peraturan/ketentuan-ketentuan tertentu dengan suatu bentuk penderitaan yang bersifat khusus yaitu berupa hukuman"[16]

Definisi yang terkenal dari pakar hukum Indonesia Moeljatno mengenai hukum ialah Hukum Pidana itu adalah bagian dari keseluruhan hukum yang menjadi dasar-dasar dan aturan-aturan mengenai:[17]

- Penetapan-penetapan mengenai perbuatan-perbuatan mana yang tidak boleh dilakukan atau yang boleh dilakukan, lalu perbuatan mana yang dilarang, dan perbuatan mana yang diancam hukuman atau sanksi pidana tertentu bagi barang siapa yang melakukan pelanggaran atas larangan-larangan tersebut.
- Penetapan-penetapan mengenai hal apa saja bagi mereka yang telah melanggar larangan-larangan itu dapat dikenakan padanya hukuman pidana sebagaimana yang diancamkan kepadanya.
- Petetapan-penetapan mengenai bagaimana cara pengenaan pidana itu diberlakukan dan dilaksanakan apabila seseorang yang disangkakan melanggar larangan tersebut.

---

[15] Moeljatno, *Asas-Asas Hukum Pidana*, Cetakan Ke-lima, Rineka Cipta, Jakarta, 1993, h. 16

[16] *Ibid*

[17] Moeljatno, Op.cit, h. 1

Pada dasarnya tujuan hukum itu baik privat maupun publik adalah hal-hal yang cakupannya adalah mengandung keadilan, kemanfaatan, dan kepastian hukum, berdasarkan skala prioritas yang sepadan dengan kasus atau permasalahan yang sedang dihadapi atau hendak dipecahkan.

Hukum pidana disebut sebaga hukum publik, yang artinya hukum yang mengatur kepentingan umum yaitu hubungan antara negara dan orang-perorang. Pengertian tersebut memberikan kesimpulan bahwa hal-hak yang dibahas dalam hukum pidana pada dasarnya ada 3 yaitu; (1) Perbuatan Pidana, (2) Pertanggungjawaban Pidana, (3) Sanksi Pidana.

Subjek Hukum Pidana sendiri adalah "orang", namun dalam perkembangannya Subjek Hukum tidak lagi hanya "orang" melainkan juga berbagai macam bentuk badan hukum, walaupun tentu saja yang dipertanggungjawabkan tentu "orang" yaitu para pengurus dari Badan Hukum tersebut, karena pada prinsipnya tujuan diadakannya sanksi pidana adalah bermanfat untuk orang. Badan hukum Korporasi dapat menjadi Subjek hukum pidana karena korporasi adalah sebuah figur hukum yang memiliki kewenangan melakukan perbuatan hukum yang diakui oleh hukum perdata. Badan hukum korporasi juga memiliki peran penting sebagai "pelaku" sosial dalam kehidupan bermasyarakat seiring dengan semakin kompleks dan berkembangnya kemajuan kehidupan masyarakat. Untuk itu pengaturan Korporasi sebagai Pelaku tindak pidana harus lah jelas agar ketika pelanggaran hukum terjadi dan sanksi pidana diterapkan maka pengurus anggota-anggota badan pengurus atau komisaris-komisaris yang

terlibat dalam suatu tindak pidana kejahatan harus tepisah beban pertanggungjawabannya dengan mereka yang ternyata tidak ikut campur dalam pelanggaran itu, sehingga keadilan dapat ditegakkan.

Konsekuensi yang bersifat nestapa atau kesusahan yang diberlakukan atau diancamkan atau dikenakan terhadap seseorang karena perbuatannya disebut sanksi pidana. Memberikan ganjaran kepada pelaku tindak pidana yang mengganggu atau membahayakan kepentingan hukum adalah tujuan pemberian sanksi pidana. Pada prinsipnya sanksi pidana adalah sebagai penjamin dalam fungsinya merehabilitasi si pelaku kejahatan tersebut.. Sanksi pidana diciptakan sebagai suatu bentuk ancaman bagi kebebasan manusia yaitu para pelaku kejahatan. Sanksi pidana adalah bentuk hukum sebab akibat, di mana sebabnya adalah kasus yang terjadi dan akibatnya adalah hukum yang dikenakan terhadap orang yang memperoleh sanksi tersebut, baik masuk penjara ataupun terkena hukuman lain.

Hukum dibuat dengan sasaran atau tujuan tertentu yang hendak dicapai. Tujuan hukum sendiri adalah bentuk pencapaian yang ingin diwujudkan dengan menggunakan hukum sebagai alat untuk mewujudkan tujuan hukum tersebut yaitu dengan cara mengatur tatanan kehidupan suatu masyarakat. Dalam membuat suatu hukum, fungsi dari tujuan hukum itu sendiri akan membagi hak dan kewajiban antara setiap individu di dalam bermasyarakat. Dalam pergaulan hidup manusia, hak atau kepentingan-

kepentingan manusia bisa senantiasa bertentangan satu dengan yang lain, maka tujuan hukum adalah untuk melindungi hak dan kewajiban tersebut.

Tujuan pemidanaan dari waktu ke waktu berkembang. Tujuan pemidanaan pada masa ini telah menjurus ke arah yang lebih rasional dan logis. Tujuan pidana yang berlaku pada masa ini adalah berbagai variasi dari bentuk- bentuk pemidanaan yang memberikan efek penjeraan (*deterrent*), baik bagi si pelanggar hukum maupun bagi mereka yang berpotensi menjadi pelaku kejahatan. Jadi tujuan pidana bukan lagi sekedar bentuk pembalasan (*revenge*) atau tujuan pemuasan dendam. Pemidanaan bukan hanya semata-mata berbicara mengenai sanksi yang dijatuhkan tetapi juga mengenai proses atau prosedur penjatuhan sanksi berserta hukum yang mengatur baik secara materil maupun formil yang berkaitan dengan hal tersebut.[18] Tujuan pidana yang sesungguhnya adalah memperbaiki kerusakan-kerusakan individual dan sosial yang diakibatkan oleh suatu tindak kejahatan pidana. Sementara itu tujuan pemidanaan tersebut adalah[19]:

(a) melakukan pencegahan yang bersifat umum dan khusus,

(b) melakukan perlindungan terhadap publik / masyarakat,

(c) melakukan pemeliharan "rasa" solidaritas masyarakat,

(d) bentuk pengimbalan/pengimbangan;

1.5.1.2. Kepastian Hukum

[18] Barda Narwi, Kapita Selekta Hukum Pidana,
[19] *Ibid*

L.J. Van Apeldoorn seorang ahli hukum dengan bukunya terkenal *"Inleiding tot de Studie van het Nederlandse"* berpendapat, pengertian kepastian hukum adalah kepastian suatu undang-undang. Namun ternyata realitasnya sering kali kepastian hukum tidak menciptakan keadilan oleh karena nilai pasti dalam undang-undang mewajibkan hal yang tentu, sedangkan kepentingan manusia/penduduk tidak pernah pasti.[20] Secara normatif kepastian hukum adalah ketika suatu peraturan atau ketentuan apapun yang dibuat, diundangkan dan diaplikasikan secara nyata dan menunjukkan aturan/ketentuan yang jelas dan logis dan tidak menimbulkan keragu-raguan atau multi tafsir. Jadi kepastian hukum yang dimaksud adalah rangkaian dalam sistem norma hukum yang tidak berbenturan dengan peraturan lain dan menimbulkan konflik norma.

Sebagaimana dikatakan oleh pakar hukum Rochmat Soemitro, kepastian hukum adalah bentuk keadilan yang merupakan kepastian hukum yang diwujudkan dalam bentuk undang-undang untuk mengakomodasi nilai-nilai keadilan.[21] Kepastian hukum adalah *certainty* dari keseluruhan tujuan bagi setiap undang-undang yang berlaku. Undang-undang dan peraturan-peraturan yang mengikat umum harus memberikan ketegasan dan kejelasan sehingga tidak memberikan pengertian ganda atau penafsiran yang berbeda-beda. Dalam penerapannya setiap ketentuan peraturan perundang-undangan, apabila terbentur pada pilihan keadilan atau kepastian

[20]L.J. Van Apeldoorn, *Pengantar Ilmu Hukum*, Terjemahan, Diterjemahkan Oleh: Oetarid Sadino, (Jakarta: Pradnya Paramitha, 2009), h. 15.

[21] Rochmat Soemitro, *Asas-asas dan Dasar Perpajakan*, (Bandung: Refika Aditama, 2004), h. 21.

hukum, maka yang lebih diutamakan harusnya yang mewujudkan kepastian hukum karena ”tujuan hukum itu sendiri tidak lain adalah untuk menciptakan ketertiban melalui kepastian hukum”.

Kepastian hukum banyak bergantung pada rangkaian susunan kalimat, susunan kata, dan istilah-istilah baku yang dipakai. Untuk mencapai tujuan dari hukum tersebut maka digunakan bahasa hukum secara jelas dan tepat. Bahasa Indonesia adalah bahasa hukum Indonesia, oleh karena itu kepastian hukum juga banyak bergantung kepada penggunaan bahasa Indonesia yang bertatabahasa baik dan benar, yaitu bahasa Indonesia yang aturannya sesuai dengan norma-norma bahasa yang sudah baku. Asas-asas hukum yang bersifat universal dan diterima secara umum sangat dipentingkan dalam penyusunan undang-undang yang baik sebagaimana berikut ini:[22]

1. *Lex specialis derogat lex generalis*; asas ini mengatakan bahwa hukum yang bersifat khusus (atau disebut *lex specialis*) akan mengenyampingkan hukum yang bersifat umum (atau disebut *lex generalis*).
2. *Lex posterior derogat lex priori*; merupakan asas yang menyatakan bahwa hukum yang terbaru (*posterior*) akan mengesampingkan hukum yang lama /sebelumnya (*prior*).
3. *Pacta sunt servanda*, merupakan asas yang menyatakan ketegasan makna Perjanjian yang dikenal sebagai berikut; “setiap bentuk

[22]*Ibid.*

perjanjian adalah hukum yang mengikat bagi para pihak yang melakukan perjanjian / yang menandatanganinya".

4. *Lex locus contractus*, Sebuah kontrak ditentukan dimana kontrak itu diciptakan/dibuat/dilahirkan. Demikian asas Lex Locus Contractus mengatakan.
5. *Nulla poena sine privilegia lege*, disebut juga asas legalitas.
6. Asas Non Diskriminasi, merupakan asas yang tidak membedakan perlakuan warga negara mengenai segala sesuatu yang berkaitan dengan dasar suku, ras, agama, golongan dan gender.
7. Domisili, sumber, kebangsaan, yaitu asas negara tempat tinggal seseorang, negara yang menjadi tempat sumber penghasilan seseorang, dan asas nationalitiet.
8. Asas keajegan; merupakan asas yang menegaskan tentang suatu kondisi keteraturan sosial yang tetap dan tidak berubah sebagai hasil hubungan yang selaras/sepadan antara tindakan, norma, dan nilai-nilai dalam interaksi sosial.
9. Asas kontinuitas; merupakan asas yang menjamin keberlangsungan berlakunya sesuatu keputusan sebuah lembaga/instansi/organisasi, meskipun si pejabat yang menandatangani berganti.
10. Asas keadilan; Disebut juga asas tanpa pengecualian atau asas yang menekankan bahwa setiap materi muatan peraturan perundang-undangan harus mencerminkan keadilan yang murni dan berlaku bagi bagi setiap Warga Negara tanpa terkecuali.

Mengenai kriteria kepastian hukum, Satjipto Rahardjo memberikan pendapatnya apa itu kriteria kepastian hukum dengan pernyataan sebagai berikut: "Hukum itu adalah sebuah institusi yang tujuan pokoknya adalah mengantarkan/membawa manusia secara ideal, kepada kehidupan yang adil, yang sejahtera dan yang pastinya membuat manusia bahagia."[23] Pernyataan tersebut adalah pokok pikiran yang akhirnya menuntut kehadiran hukum progresif dan melahirkan bentuk hukum baru yaitu "hukum progresif". Juga mengandung keyakinan mengenai hukum, baik dari sudut fungsi, konsep, maupun tujuannya. Hal itu lah yang disebut sebagai ideal hukum yang menuntut perwujudannya dalam kehidupan manusia. Hukum akhirnya menjadi suatu proses yang tidak berhenti membangun dirinya menuju ideal hukum tersebut. Inilah esensi pokok dari hukum progresif.[24]

Pendapat Satjipto Rahardjo bertentangan dengan pendapat L.J. van Apeldoorn maupun Rochmat Soemitro. Kepastian hukum bukan lah suatu bentuk kristalisasi keadilan. Kepastian undang-undang bukan berarti juga disitu letak kepastian hukum. Hukum akan selalu diliha dan dibicarakan dari perspektif kepastian hukum dan itulah sebabnya kepastian hukum adalah sentra utama dalam setiap pembicaraan dengan sujek hukum. Jadi kepastian hukum itu adalah produk dari hukum itu sendiri atau lebih khusus dari apa

[23]Satjipto Rahardjo, *Hukum Progresif, Sebuah Sintesa Hukum Indonesia*, (Yogyakarta:Genta Publishing, 2009), h. 2

[24]*Ibid.h.13*

yang kita debut sebagai perundang-undangan. Begitu datang hukum, maka datanglah yang disebut KEPASTIAN.

Menurut Satjipto Rahardjo, beban yang sangat berlebihan ini seharusnya tidak dipikul di pundak hukum. Lebih dari itu, pemahaman dan keyakinan yang terlalu besar seperti itu, akan memberikan kesempatan besar untuk menyesatkan, karena seolah kepastian hukum sudah terbentuk sedemikian rupa menjadi ideologi dalam hukum. [25]

1.5.2. Kerangka Konsep

Tindak pidana kejahatan adalah suatu perbuatan yang oleh hukum dilarang dan diancam dengan pidana yang berlaku bagi barang siapa pun yang melanggar larangan-larangan tersebut.

Cybercrime adalah suatu terminologi yang mengacu kepada aktivitas tindak kejahatan yang dilakukan dengan komputer atau jaringan komputer yang dijadikan sebagai alat, sebagai sasaran kejahatan atau sebagai tempat terjadinya kejahatan.

Transnational cybercrime adalah kejahatan-kejahatan yang sebenarnya terjadi di dalam satu batas wilayah negara tertentu, tetapi ada bagian-bagian dari kejahatan tersebut yang terkait dengan negara-negara lain, sehingga terlihat adanya keterlibatan dua atau lebih negara yang berkepentingan atau yang terkait dengan kejahatan itu.

[25] Satjipto Rahardjo, *Hukum Progresif, Sebuah Sintesa Hukum Indonesia*, (Yogyakarta:Genta Publishing, 2009), h. 6

Transnational cybercrime merupakan bentuk pengembangan karakteristik dari bentuk kejahatan kontemporer yang disebut sebagai *Organized crime* yaitu kejahatan terorganisir yang dimulai sekitar tahun 1970. Bentuk kejahatan itu sendiri sebenarnya sudah menjadi "*concern*" semua negara di dunia karena peningkatan kualitas dan kuantitas kejahatan tersebut berkembang menjadi organisasi kejahatan transnasional yang menembus batas batas negara dan menunjukkan adanya Kerjasama kejahatan antara negara yang menjadikan kejahatan international semakin marak.

Kerangka konsep akan menggambarkan bagaimana kejahatan komputer dilakukan dengan perencanaan yang matang oleh para pelakunya dan juga membutuhkan perencanaan yang matang juga dalam membongkar atau mengungkapkannya. Kerangka konsep juga akan menggambarkan bagaimana pentingnya hubungan bilateral antar negara dalam menghadapi dampak globalisasi terhadap tingkat kejahatan transnasional ini.

Seseorang yang karena perbuatannya atau keadaan yang dibuatnya, berdasarkan bukti permulaan yang cukup patut diduga atau dapat dikatakan sebagai pelaku tindak pidana disebut sebagai Tersangka. . Seseorang yang diduga kuat telah melakukan tindak pidana, kepadanya dapat dilakukan perintah penangkapan berdasarkan bukti permulaan yang sesuai dengan perundangan yang berlaku. Dalam suatu penetapan tersangka baik pada kejahatan konvensional maupun *cybercrime* harus didapati bukti permulaan yang cukup yaitu paling sedikit 2 (dua) jenis alat bukti yang ditentukan

melalui gelar pekara. Dalam Penetapan Tersangka juga harus ada proses yang dilalui terlebih dahulu. Sama seperti kejahatan konvensional, pada kejahatan dunia maya diperlukan proses khusus sebelum penetapan tersangka pelaku kejahatan siber, apa lagi jika dilakukan dengan melibatkan beberapa negara seperti tindak pidana *transnational cybecrime*.

1.6 Metode Penelitian

Metode penelitian yang digunakan adalah:

1.6.1 Tipe Penelitian

Penelitian tesis ini bersifat yuridis normative. Penyusunan penelitian ini dibuat dengan memberikan pemahaman terhadap permasalahan dengan meneliti bahan sekunder atau bahan-bahan Pustaka. Penelitian ini juga memberikan analisis terhadap masalah norma yang dialami oleh hukum dogmatif dan kegiatan mendeskriptifkan norma hukum itu dirumuskan dengan norma hukum (membentuk peraturan perundangan). Penelitian yuridis normatif ini juga dihubungkan dengan fakta-fakta yang secara nyata terjadi dalam pelaksanaan peraturan perundang-undangan serta asas-asas hukum dan teori-teori hukum dan praktek di dalam penetapan tersangka dalam tindak pidana *transnational cybercrime.*

1.6.2. Objek Penelitian

a). Pengaturan penetapan tersangka secara umum dalam hukum positif

b). Pengaturan penetapan tersangka *cybercrime* dan *transnational cybercrime*

1.6.3. Jenis Data

Jenis data yang akan Penulis gunakan dalam penelitian ini diperoleh dari Kitab Undang-undang Hukum Pidana (KUHP), Kitab Undang-undang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), juga Ketentuan *Convention On Cybercrime 2001* yang terkait dengan Hukum Positif Indonesia. Data-data sekunder yang menjadi bahan rujukan peulisan ini diperoleh Penulis dari bahan-bahan kepustakaan berupa dokumen-dokumen hukum, buku-buku, jurnal-jurnal, makalah, berita berita online dan lain-lain. Secara khusus Penulis melakukan wawancara dengan KANIT IV, Subdit III DittipidSiber, Bareskrim MABES POLRI untuk mengetahui langsung bagaimana penetapan Tersangka ini terjadi pada prakteknya di lapangan, dan kendala apa saja yang dihadapi. Demikian pula mengenai data Tertier akan penulis peroleh dari berbagai dictionary termasuk dictionary hukum juga kamus-kamus, ensiklopedia, dan berbagai data yang berfungsi sebagai pendukung data primer dan data sekunder.

1.6.4. Spesifikasi Penelitian

Penulis memilih penelitian deskriptif sebagai spesifikasi penelitian ini. Penelitian ini secara khusus menelaah inti dari permasalahan dalam penelitian ini dengan menggambarkan peraturan perundang-undangan yang berlaku dan dikaitkan dengan teori-teori hukum dalam praktek pelaksanaannya dan dengan demikian akan teruraikan/tergambarkan lah

fakta-fakta yang secara nyata terjadi dalam penetapan tersangka *transnational cybercrime*

1.6.5. Fokus Studi

Fokus studi dalam penelitian ini adalah terkait dengan hukum pidana, secara khusus membahas masalah Penetapan Tersangka pada kasus-kasus *transnational cybercrime* yang bertujuan agar kasus-kasus *transnational cybercrime* dapat ditangani dengan tuntas.

1.6.6. Metode Pendekatan

Penulis secara spesifik akan menggunakan metode analisis data kualitatif untuk menjawab dan memecahkan permasalahan yang ditelaah dalam penelitian ini,. Metode pendekatan yang digunakan Penulis dalam penelitian ini menggunakan pendekatan undang-undang (*statute approach*), yang artinya penulis akan meneliti dan menelaah semua undang-undang dan regulasi yang terkait dengan isi permasalahan hukum yang sedang ditangani sehingga dapat ditarik kesimpulan yang dapat dipertanggungjawabkan;

1.6.7. Teknik Pendekatan

Teknik pendekatan yang digunakan dalam penelitian ini adalah dengan *statute approach* atau biasa disebut sebagai pendekatan undang-undang. Pendekatannya menggunakan data sekunder. Pada data sekunder, yaitu data yang diperoleh langsung melalui penelusuran kepustakaan atau dari dokumen resmi termasuk juga wawancara dengan instansi yang sudah menangani penetapan tersangka yaitu Kanit IV, Subdit III Dittipidsiber Bareskrim MABES POLRI. Hal ini penting dilakukan, tujuannya agar

Penulis memilah-milah data yang ada dan kemudian menganalisisnya berdasarkan pada peraturan/ketentuan perundang-undangan.

1.6.8. Metode Pengolahan

Sebagai upaya untuk dapat menjawab atau memecahkan masalah dalam penelitian ini, Penulis akan menggunakan metode analisis data kualitatif, karena data yang diperoleh bersifat kualitas bukan kuantitas. Setelah pengumpulan data maka selanjutnya akan dilakukan pengolahan data dan analisis secara kualitatif, sehingga dapat ditarik kesimpulan yang dapat dipertanggungjawabkan

1.6.9. Teknik Penyajian Data

Data yang telah diuraikan tersebut kemudian akan disajikan secara deskriptif dengan metode deduktif sehingga dapat diperoleh kejelasan penyelesaian apatyang dari sana dapat ditarik kesimpulan atas hal-hal yang bersifat umum menuju ke hal yang lebih khusus.

1.7. Sistematika Penulisan

Penulisan ini menggunakan sistematika sebagai berikut:

BAB I PENDAHULUAN

Pada Bab Pendahuluan ini akan dijabarkan uraian dan latar belakang permasalahan, perumusan masalah, maksud dan tujuan penelitian, kerangka teoritis dan konsep, metode penelitian dan sistematika penelitian.

BAB II *TRANSNATIONAL CYBERCRIME* DAN PENETAPAN TERSANGKA

Bab ini berisi tinjauan umum dan teori-teori tentang Tindak Pidana, Alat -alat Bukti dalam Hukum Pidana, lalu Penulis juga akan mengulas lebih dalam mengenai *teori* Yurisdiksi, Perspektif Hukum Progresif, dan Kepastian Hukum serta teori-teori yang berhubungan dengan Penetapan Tersangka dalam *transnational cybercrime*

BAB III KASUS-KASUS *CYBERCRIME* DALAM KEJAHATAN TRANS NASIONAL DI INDONESIA

Bab ini berisi mengenai analisis terhadap permasalahan konstruksi yuiridis penetapan tersangka dalam tindak pidana *transnational cybercrime* dalam hukum positif

BAB IV PERBANDINGAN PENANGANAN PENETAPAN TINDAK PIDANA TRANSNATIONAL CYBERCRIME DI INDONESIA DENGAN AMERIKA SERIKAT DAN INGGRIS

Berisi pembahasan bagaimana perbandingan penegakkan hukum dan penanganan tindak pidana *transnational cybercrime* di Indonesia dengan Amerika Serikat dan Inggris

BAB V PENUTUP

Berisi kesimpulan dan saran-saran sebagai intisari dari Tesis ini.