BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Kejahatan bukanlah konsep baru dalam sejarah peradaban manusia. Pada tahapan perkembangannya modus operandi kejahatan bergerak maju seiring perkembangan peradaban manusia. Kejahatan dan eksistensi masyarakat dalam teknologi informasi seperti internet menjadi "dua sisi mata uang" yang saling terkait karena selain internet memberikan kemajuan teknologi, sekaligus dapat menjadi sarana perbuatan melawan hukum.[1] Kejahatan merupakan salah satu sifat fitrah manusia yang ada pada diri manusia dan terus mengalami perkembangan signifikan sesuai dengan perkembangan masyarakat itu sendiri. Semakin meningkatnya perkembangan teknologi informasi, maka akan semakin meningkat juga modus para individu dalam melakukan kejahatannya.

Kejahatan siber merupakan salah satu kejahatan baru yang terus mengalami perkembangan baik dari sisi modus operandi maupun ragam kejahatannya. Lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) memberikan asa bahwa persoalan-persoalan dibidang hukum telematika perlahan pasti akan dapat terjawab.[2] Meskipun disadari bahwa masih terdapat kekurangan yang ditemukan dalam Undang-Undang tersebut. Undang-Undang ini dapat dipandang sebagai momentum positif dalam penanganan sengketa-sengketa dibidang telematika, sehingga harus tetap

---

[1]Maskun, 2013, *Kejahatan Siber (cyber crime),* Jakarta, Kencana, hlm. 2.
[2]*Ibid*

direspons positif dengan memberikan berbagai kritik membangun menuju kesempurnaan ketentuan hukum nasional Indonesia tentang hukum telematika.

Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) menyebutkan bahwa:

1. Setiap orang dengan sengaja dan tanpa hak ata melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun.
2. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3. 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.[3]

Konstruksi Pasal 30 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) menyebutkan bahwa tindak ilegal yang dilakukan seseorang terhadap sistem elektronik orang lain dengan tujuan untuk memperoleh informasi/dokumen elektronik dan/atau upaya pembobolan, penerobosan, dan penjebolan yang melanggar dan melampaui sistem pengamanan adalah sesuatu yang terlarang. Beberapa kasus yang relevan dan telah terjadi dalam praktik dunia siber dapat dilihat pada kasus pembobolan kartu kredit,

---

[3] *Ibid*, hlm. 36.

pembobolan situs KPU 2004, penjebolan beberapa dokumen penting pada Departemen Pertanahan dan Keamanan Pemerintah Amerika Serikat, dan masih banyak lagi contoh kasus lainnya yang harus diselesaikan dengan menggunakan aturan hukum yang belum secara khusus mengatur tentang bentuk kejahatan/pelanggaran yang dimaksud.[4]

Internet telah membawa manfaat besar bagi manusia. Pemanfaatannya tidak saja dalam pemerintahan, dunia swasta/perusahaan, akan tetapi sudah menjangkau pada seluruh sektor kehidupan termasuk segala keperluan rumah tangga (pribadi). Akan tetapi, kemajuan teknologi informasi (internet) dan segala bentuk manfaat di dalamnya membawa konsekuensi negatif tersendiri dimana semakin mudahnya para penjahat untuk melakukan aksinya yang semakin merisaukan masyarakat. Sekarang ini sedang sering terjadi kejahatan yang dilakukan dengan pembobolan melalui sistem bank yaitu internet banking yang dianggap memudahkan bagi para nasabah bank dalam melakukan transaksi, tetapi dibalik kemudahan tersebut ada juga kekurangan yaitu dapat terjadinya pembobolan oleh para hacker.[5]

Internet banyak dipergunakan dalam kegiatan Perbankan di berbagai negara contohnya seperti internet banking. Dengan disediakannya fasilitas layanan internet banking, nasabah mendapat keuntungan berupa fleksibilitas untuk melakukan kegiatannya setiap saat. Internet banking memiliki manfaat positif contohnya :

---

[4] *Ibid*

[5] Dina Nhakha, 2013, *"Perlindungan Nasabah Bank dalam Penggunaan Fasilitas Internet Banking atas terjadinya Cyber Crime"*, http://dina-nhakha.blogspot.com/2013/06.html, diakses 15 Oktober 2013 (17.00).

1. Cek saldo dan melihat transaksi terakhir Anda hingga 90 hari.
2. Membuka dan mengatur Rekening Tambahan dan Deposito Berjangka.
3. Transfer dana antar bank di Indonesia menggunakan layanan SKN atau RTGS.
4. Transfer dana ke luar negeri.
5. Layanan Pembayaran dan Pembelian.
6. Pengaturan batas transaksi harian.[6]

Transaksi internet banking juga berpotensi mengalami kegagalan atau menjadi objek kejahatan elektronik, seperti kejahatan siber atau sering disebut *cyber crime.* Beberapa Undang-Undang yang mengatur tentang internet banking misalnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.[7] Internet banking merupakan salah satu pelayanan perbankan tanpa cabang yaitu berupa fasilitas yang akan memudahkan nasabah untuk melakukan transaksi perbankan tanpa perlu datang ke kantor cabang. Meskipun demikian, dalam setiap kemudahan pasti terdapat sebuah resiko yang harus diperhatikan. Tidak sedikit nasabah yang masih ragu menggunakan fasilitas *internet banking* karena merasa teknologi yang diterapkan oleh pihak perbankan tidak cukup mutakhir sehingga meragukan keamanannya. Selain itu masih banyak nasabah yang tidak teredukasi dengan baik dalam menggunakan internet secara aman sehingga mereka takut

---

[6] *Ibid*
[7] *Ibid*

menjadi korban. Hal tersebut semakin menambahkan keraguan pada nasabah untuk menggunakan fasilitas tersebut.

Pengaturan internet banking tentu saja tidak terlepas dari Undang-Undang Perbankan Nomor 7 Tahun 1992 jo Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Yang perlu diperhatikan dalam permasalahan ini yaitu bagaimana yang dapat diberikan untuk mencegah dan menanggulangi akibat dari penyelenggaraan internet banking. Peraturan perundangan tersebut yang dapat dikaitkan dengan internet banking misalnya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Di dalam Undang-Undang ini bahkan tidak ada Pasal yang jelas-jelas mengatur tentang internet banking. Akan tetapi, ada pasal yang mengatur tentang transaksi dengan media internet.[8]

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) telah menjadi acuan bagi penyelenggaraan kegiatan transaksi elektronik, yang diselenggarakan oleh bank. Resiko yang biasanya dialami dalam sistem internet banking adalah resiko kekeliruan pada tahap pengoperasian, resiko akses oleh pihak yang tidak berwenang, resiko kehilangan atau kerusakan data.[9] Berbagai upaya preventif memang telah diterapkan oleh kalangan perbankan di Indonesia yang menyelenggarakan layanan internet banking. Misalnya, dengan diberlakukannya fitur bukti otentik kedua (*two factor authentication*) yang menggunakan *token*. Penggunaan *token* ini akan memberikan keamanan yang

---

[8] *Ibid*

[9] Yudicare, 2011, "*Tanggungjawab bank terhadap potensi risiko kegagalan sistem dan atau risiko kejahatan elektronik cybercrime pada internet banking*", http://yudicare.wordpress.com/2011/03/28.html, diakses 15 Oktober 2013 (17.00)

lebih tinggi dibandingkan bila hanya menggunakan nama nasabah pengguna layanan internet banking (*username*), PIN, dan *password* saja. Akan tetapi dengan adanya penggunaan *token* ini, tidak berarti transaksi internet banking bebas dari resiko.[10]

Dengan adanya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) ini, maka apabila ada pihak-pihak tertentu yang menyalahgunakan media internet dalam transaksi perbankan, dan terjadi permasalahan ataupun sengketa berkaitan dengan internet banking dan diatur dalam undang-undang ini, maka dapat diselesaikan atau diproses dengan berdasarkan pada ketentuan-ketentuan dalam undang-undang ini. Selain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi juga dapat dikaitkan dengan internet banking, mengingat bahwa penyelenggaraan internet banking pada dasarnya tidak terlepas dari penggunaan jasa telekomunikasi.[11]

Layanan internet banking adalah pemanfaatan teknologi internet sebagai media untuk melakukan transaksi Perbankan yang menggunakan jaringan internet sebagai perantara antara nasabah dan pihak bank. Bentuk transaksinya bersifat maya atau tanpa proses tatap muka antara nasabah bank dan petugas bank yang bersangkutan.[12] Internet banking merupakan kebalikan dari proses transaksi perbankan konvensional, dimana pada proses transaksi konvensional diperlukan tatap muka langsung antara pihak bank dan juga nasabah, maka hal itu tidak

---

[10] *Ibid*

[11] *Ibid*

[12] Michael Yohanes, 2011, *"Pengertian Internet Banking"*, http://Michael yohanes.blogspot.com/2011/11/pengertian_internet_banking.html, diakses 27 November 2013 (14.30).

diperlukan jika kita menggunakan layanan internet banking ketika melakukan transaksi perbankan. Transaksi yang dilakukan pun bersifat maya, artinya semua transaksi dilakukan dengan dukungan koneksi internet dan tanpa tatap muka langsung dengan pihak bank.

Dengan bermodalkan koneksi internet yang kita miliki, baik itu melalui PC, telefon genggam, maupun tablet, transaksi internet banking pun dapat kita lakukan dimanapun. Contoh kasus *cyber crime* di Indonesia yaitu pencurian dan penggunaan account internet milik orang lain. Salah satunya ISP yang dicuri dan digunakan secara tidak sah, pencurian ini cukup menangkap *User ID* dan *Password* saja.

B. Rumusan Masalah

1. Apa modus tindak pidana *cyber crime* (kejahatan siber) pada internet banking?
2. Apa peraturan yang dapat diterapkan terhadap terjadinya *cyber crime* (kejahatan siber) pada internet banking?

C. Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah sebagai berikut:

1. Untuk mengetahui dan mengkaji modus tindak pidana *cyber crime* (kejahatan siber) pada internet banking.
2. Untuk mengetahui dan mengkaji peraturan yang dapat diterapkan terhadap terjadinya *cyber crime* (kejahatan siber) pada internet banking.

D. Tinjauan Pustaka

1. Pengertian *Cyber crime* (Kejahatan Siber)

Pengertian tindak pidana *cyber crime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet. *Cyber crime* adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama dan memanfaatkan internet. Istilah *cyber crime* diambil dari bahasa inggris yang artinya kejahatan dunia maya, karena aktifitas kejahatan menggunakan komputer maupun jaringan komputer untuk dijadikan sarana atau tempat transaksi terjadinya kejahatan. *Cyber crime* merupakan tindak pidana yang dilakukan pada teknologi internet (*cyber space*), baik itu menyerang fasilitas umum di dalam *cyber space* maupun data pribadi yang bersifat penting maupun yang dirahasiakan.[13] Tindakan ini masing-masing memiliki karakteristik sendiri, namun juga memiliki perbedaan utama dari tindakan tersebut adalah keterkaitan dengan menggunakan jaringan informasi publik (internet). *Cyber crime* diklasifikasikan menjadi tiga yaitu:

a. *Cyberpiracy* merupakan penggunaan teknologi komputer untuk mencetak ulang software atau informasi kemudian mendistribusikan informasi atau software tersebut melalui teknologi komputer. Dapat dikatakan sebagai pembajakan software secara ilegal.
b. *Cybertrespass* merupakan penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau individu. Misalnya hacking, exploit system dan seluruh kegiatan yang berhubungan dengan akses pada sistem komputer tersebut.

[13] http://Roniamardi.wordpress.com/definisi cyber crime.html, diakses 27 November 2013 (14.30).

c. *Cybervandalism* merupakan penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik dan menghancurkan data di sistem komputer. Contohnya virus, trojan worm, metode DoS, Http Attack, BruteForce, dan lain-lain.[14]

2. Internet Banking

Internet banking adalah melakukan transaksi, pembayaran, dan transaksi lainnya melalui internet dengan website milik bank yang dilengkapi sistem keamanan.[15] Adapun kemudahan dari sistem internet banking antara lain :

a. Aplikasi mudah digunakan.
b. Layanan dapat dijangkau dari mana saja.
c. Murah.
d. Dapat dipercaya.
e. Dapat diandalkan

Layanan internet banking adalah pemanfaatan teknologi internet sebagai media untuk melakukan transaksi perbankan yang menggunakan jaringan internet sebagai perantara antara nasabah dan pihak bank. Bentuk transaksinya bersifat maya atau tanpa proses tatap muka antara nasabah bank dan petugas bank yang bersangkutan.[16] Dengan kata lain internet banking merupakan kebalikan dari proses transaksi perbankan konvensional, dimana pada proses transaksi konvensional diperlukan tatap muka antara langsung antara pihak bank dan juga

[14]http://yonalisa.blogspot.com/2012/10/klasifikasi-cyber-crime_24.html, diakses tanggal 12 Maret 2015 (08.30)
[15]Ilham Dinar, 2012, *"Internet Banking"*, http://Ilham dinar18.blogspot.com/2012/10/internet banking.html, diakses 27 November 2013 (14.30).
[16]Michael Yohanes, 2011, *"Pengertian internet banking"*, http://Michaelyohanes.blogspot.com/2011/11/pengertian internet banking.html, diakses 27 November 2013 (14.30).

nasabah, maka hal itu tidak diperlukan jika kita menggunakan layanan internet banking ketika melakukan transaksi perbankan. Transaksi yang dilakukan pun bersifat maya, artinya semua transaksi dilakukan secara

nasabah, maka hal itu tidak diperlukan jika kita menggunakan layanan internet banking ketika melakukan transaksi perbankan. Transaksi yang dilakukan pun bersifat maya, artinya semua transaksi dilakukan dengan dukungan koneksi internet dan tanpa tatap muka langsung dengan pihak bank. Dengan bermodalkan koneksi internet yang kita miliki, baik itu melalui PC, telefon genggam, maupun tablet, transaksi internet banking pun dapat kita lakukan dimanapun. Saat ini hampir semua bank di Indonesia telah memiliki layanan internet banking. Berbagai macam transaksi pun dapat dilakukan secara online. Berikut beberapa manfaat dan keuntungan internet banking :

a. Cek saldo

Apabila ingin melihat jumlah saldo yang kita miliki tidak perlu jauh-jauh datang ke bank atau ATM, cukup dengan memanfaatkan fasilitas internet banking maka kita sudah bisa mengetahui jumlah saldo yang ada di rekening kita dimana saja kita berada.

b. Pembayaran tagihan

Saat ini kita cukup mengakses akun kita melalui komputer ataupun telefon genggam untuk membayar tagihan kita sehari-hari seperti listrik, air, telefon, pulsa, tagihan sekolah anak dan lainnya yang tentu saja sudah terintegrasi dengan pihak bank. Dengan proses yang cepat, maka pembayaran tagihan pun sudah bisa dilaksanakan tanpa harus datang langsung ke tempat pembayaran seperti biasa.

c. Transfer uang non tunai

Jika biasanya kita mendatangi ATM terdekat untuk melakukan transfer, maka dengan layanan internet banking kita cukup mengakses rekening kita melalui komputer maupun telefon, cukup dengan menuliskan nominal yang ingin kita transfer dari rekening kita ke rekening yang dituju, maka uang pun sudah berpindah secara cepat.

d. Pemesanan tiket

Suatu saat kita berniat melakukan perjalanan menggunakan pesawat ataupun kereta api dan malas mengantri untuk membeli tiket, saat ini hal tersebut bisa dilakukan sambil asyik menonton televisi atau sambil membaca koran. Dengan memanfaatkan layanan internet banking, pemesanan tiket baik itu pesawat maupun kereta api bisa dilakukan tanpa harus datang ke bandara ataupun stasiun terdekat.

Kejahatan siber yang terjadi di Indonesia sudah sangat banyak terjadi. Walaupun sudah ada peraturan yang mengatur tetapi pelaku belum juga jera. Contohnya seperti kasus pada internet banking PT Bank Central Asia (BCA), pada tahun 2001 dunia Perbankan dikejutkan dengan ulah Steven Haryanto yang membeli domain serupa dengan domain resmi milik bank BCA http://www.klikbca.com dimana isinya mirip dengan situs yang dimiliki BCA. Steven Haryanto sendiri bukan ahli elektro maupun informatika, melainkan Insinyur Kimia ITB Bandung dan juga merupakan karyawan media online satunet.com.[17]

[17] http://protechdroids.wordpress.com/2014/06/01/kasus-cybercrime-phissing-di-indonesia/html. diakses 4 November 2014 (22.17)

Domain-domain yang dimiliki Steven adalah www.clickbca.com, www.klikbca.comwww.klikbca.comwww.klickbca.com. Steven murni melakukan hal itu atas dasar keingintahuan mengenai seberapa banyak orang yang tak sadar menggunakan situs klikbca.com, sekaligus menguji tingkat keamanan situs tersebut. Awalnya motivasi Steven adalah agar semua orang menjadi melek terhadap masalah keamanan dari layanan internet banking. Namun munculnya *website* "tandingan" buatan Steven tersebut membuat banyak nasabah BCA yang "kesasar" masuk ke *website* yang salah. Akibatnya lebih dari sekita 130 *user* ID dan PIN internet banking milik nasabah BCA secara otomatis terkirim pada pemilik situs BCA plesetan tersebut.[18]

Beralih dari kejahatan yang dilakukan Steven Haryanto ada pun kejahatan di bidang Perbankan khususnya dalam fasilitas internet banking yaitu tahun 1978 Stanley Mark, seorang ahli komputer, telah berhasil mengelabui Security Pacific National Bank di Los Angeles dengan sarana komputer, yaitu dengan menguasai *access* pada *data base* bank tersebut, sehingga Stanley Mark dapat mentransfer uang milik nasabah bank tersebut ke rekening pribadinya. Akibatnya bank menderita kerugian sebesar US$ 10.200.000,- hanya dalam waktu beberapa menit.[19]

Tahun 1986, dari sebuah kamar hotel di New York, dua orang muda yakni Rudy Demsy dan Seno Adji berhasil mentransfer uang Bank Negara Indonesia 1946 (BNI 1946) di Citibank dan Mantrust New York ke beberapa bank di

---

[18] *Ibid*

[19] Alexander Pattipeilahy, *Di Balik Kecanggihan sebuah Teknologi*, dalam: *Majalah Komputer dan Elektronika,* No. 5 Tahun III April 1985, halaman 42 (Dalam buku Al. Wisnubroto, 2011, *Konsep Hukum Pidana Telematika,* Yogyakarta, Universitas Atmajaya Yogyakarta, hlm. 91).

Panama, Hong Kong dan Luksemburg sebesar US $ 18.700.000,00 atau sekita 30 milyar rupiah dengan mempergunakan Personal Komputer yang dilengkapi dengan "*modem*" (alat yang memungkinkan komputer berkomunikasi dengan komputer lain yang jaraknya berjauhan). *Unauthorized Transfer* Dana Bank dari jarak puluhan kilometer itu dapat terlaksana karena Rudy Demsy adalah eks karyawan BNI 1946 cabang Citibank New York, sehingga ia mengetahui *Test Key* komputer dan *password release* komputer BNI 1946 New York Agency, lagi pula Rudy Demsy dan Seno Adji sangat menguasai pengoperasian komputer.[20]

E. Metode Penelitian

1. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian hukum normatif. Penelitian hukum normatif yaitu mencakup penelitian hukum terhadap asas-asas hukum dari peraturan perundangan, putusan pengadilan.

2. Sumber Data

Untuk mendapatkan bahan penelitian hukum, maka penelitian ini dilakukan dengan studi pustaka yang mengkaji bahan hukum. Bahan hukum sebagai bahan penelitian diambil dari bahan kepustakaan yang berupa data sekunder yang terdiri dari:

a. Bahan hukum primer yaitu bahan hukum yang mempunyai kekuatan mengikat yang berisikan peraturan perundangan yang terdiri dari:

   1) Kitab Undang-Undang Hukum Pidana (KUHP).

---

[20] "*Men-'Digger' Dana BNI 1946, Rp 30 Milyar*", Tempo, Nomor 24, Tahun XVII, 24 Oktober 1987, hlm. 34-40, (Dalam buku Al. Wisnubroto, 2011, *Konsep Hukum Pidana Telematika*, Yogyakarta, Universitas Atmajaya Yogyakarta, hlm. 95-96).

2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE).

3) Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi.

4) Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan.

b. Bahan hukum sekunder yaitu bahan hukum yang erat kaitannya dengan bahan hukum primer yang berupa pendapat hukum, ajaran (doktrin), dan teori hukum sebagai penunjang bahan hukum primer yang berupa literatur-literatur atau dokumen-dokumen yang ada kaitannya dengan tindak pidana *cyber crime* (kejahatan komputer) dan internet banking, yaitu:

1) Kejahatan Siber (*cyber crime*).

2) Tindak Pidana Teknologi Informasi (*cyber crime*).

3) Strategi Penanggulangan Kejahatan Telematika.

4) Konsep Hukum Pidana Telematika.

5) *Cyber space, Cyber crimes, Cyber law.*

6) Hukum Perlindungan Nasabah Bank.

7) Hukum Informasi dan Transaksi Elektronik.

8) *Cyber crime* Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi.

9) Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer.

10) *Cyber Law* dan HAKI dalam Sistem Hukum Indonesia

c. Bahan hukum tersier adalah bahan penelitian yang menjelaskan mengenai bahan hukum primer dan sekunder, berupa kamus hukum dan ensiklopedi yaitu Kamus Bahasa Inggris dan Kamus Bahasa Indonesia.

3. Narasumber:

a. Dr. Aloysius Wisnubroto, S.H., M.Hum, Pakar Hukum Universitas Atmajaya Yogyakarta.

b. AKP. Novita Ekasari, S.H., SIK., M.H. dan Kompol Hendri Multi, Penyidik dari Polda DIY.

4. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan dengan studi dokumen yaitu suatu penulusuran bahan penelitian yang dilakukan dengan mengumpulkan data yang terdapat dalam peraturan perundang-undangan, buku-buku, dokumen, situs internet yang berkaitan dengan permasalahan yaitu mengenai *cyber crime* (kejahatan siber) dan internet banking.

5. Teknik Analisis Data

Data primer beserta data sekunder yang diperoleh akan disusun secara sistematis. Kemudian akan dilakukan analisis atas data tersebut dengan analisis secara deskriptif yaitu dengan cara menjelaskan atau memaparkan data dalam bentuk kalimat secara sistematis yang akhirnya akan menuju pada suatu kesimpulan terhadap permasalahan mengenai tindak pidana *cyber crime* (kejahatan siber) yang marak terjadi pada layanan internet banking. Sebagaimana lahirnya Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang diharapkan bisa menangani kasus-kasus dalam dunia

telekomunikasi yang kebanyakan alat kejahatan utamanya menggunakan komputer dan internet yang ada kaitannya dengan *cyber crime* (kejahatan siber).

F. Sistematika Penulisan Hukum

Sistematika penulisan hukum yang akan digunakan dalam skripsi sebagai berikut:

BAB I Pendahuluan. Bab ini menjelaskan mengenai Latar Belakang Masalah, Rumusan Masalah, Tujuan Penelitian, Tinjauan Pustaka, Metodologi Penelitian, dan Sistematika Penulisan Hukum

BAB II. Bab ini menjelaskan mengenai pengertian dan sejarah internet banking, keuntungan penggunaan internet banking, dan keamanan intenet banking

BAB III. Bab ini menjelaskan mengenai perkembangan *cyber crime* (kejahatan siber), jenis-jenis *cyber crime* (kejahatan siber), dan dampak terjadinya *cyber crime* (kejahatan siber).

BAB IV. Bab ini menjelaskan mengenai hasil penelitian dan analisis, dalam bab ini akan menjelaskan tentang hasil penelitian mengenai apa modus *cyber crime* (kejahatan siber) pada internet banking dan apa peraturan yang dapat diterapkan dalam *cyber crime* (kejahatan siber) pada internet banking.

BAB V. Bab ini adalah bagian penutup yang berisi tentang kesimpulan dan saran dari hasil penelitian dan analisis terkait dengan *cyber crime* (kejahatan siber) pada internet banking.