BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi berbasis internet saat ini tidak hanya memberikan dampak yang positif, tetapi juga mempunyai dampak negatif. Dengan kata lain, internet selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga memunculkan permasalahan baru: dalam hal ini tindak pidana di dunia maya.[1]

Sebagaimana yang dikatakan Soerjono Soekanto, bahwa kemajuan di bidang teknologi akan berjalan bersamaan dengan perubahan-perubahan di masyarakat. Perubahan-perubahan di dalam masyarakat terutama mengenai nilai-nilai sosial, kaidah-kaidah sosial, pola-pola perilaku, organisasi, dan susunan lembaga kemasyarakatan ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan."[2]

Menghadapi dampak pergeseran nilai, norma, moral, dan kesusilaan tersebut tentu diperlukan berbagai pendekatan untuk memberi perlindungan keamanan di *cyberspace*[3] (dunia maya). Pertama, pendekatan dari sistem keamanan komputer, yaitu: *authentication* (informasi benar-benar dari orang yang dikehendaki); *integrity* (informasi pesan yang dikirim tidak dimodifikasi

---

[1] Ahmad M. Ramri dan Pager Gunung dan Indra Apriadi, "Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik", diunduh dari: http://www.scribd.com/mobile/documents/39236425, hlm. 1, pada hari Minggu, 24 Juni 2012

[2] Soerjono Soekanto, *Pokok-Pokok Sosiologi Hukum*, Rajawali Pers, Jakarta, 1980, hlm. 87-88.

[3] Istilah "cyberspace" pada awalnya muncul dalam novel fantasi ilmiah yang berjudul "Neuromacer" karya William Gibson, yang terbit pada tahun 1984.

orang yang tidak berhak); *nonrepudition* (si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut); *authority* (informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut); *confidentially* (usaha untuk menjaga informasi orang yang tidak berhak mengakses); *privacy* (data-data yang sifatnya privat); *availability* (ketersediannya yang berhubungan dengan informasi ketika dibutuhkan); dan *access control* (cara pengaturan akses kepada informasi).[4]

Kedua, pendekatan teknologi, yaitu upaya pencegahan atau penanggulangan tindak pidana dengan menggunakan teknologi. Tindak pidana *cybercrime* yang terkait erat dengan kemajuan teknologi tidak dapat semata-mata ditanggulangi dengan pendekatan yuridis, tapi juga ditanggulangi dengan pendekatan teknologi itu sendiri.

Ketiga, pendekatan yuridis, yaitu upaya yang dilakukan oleh penegak hukum dalam menegakkan keadilan; memberikan efek jera pada pelaku, dan korban dalam memperoleh keadilan.

Keempat, pendekatan budaya maupun etik, yaitu membangun atau membangkitkan kepekaan masyarakat dan aparat penegak hukum terhadap masalah *cybercrime* dengan cara menyebarluaskan atau mengajarkan etika pengguna komputer melalui pendidikan.

Terlepas dari berbagai pendekatan di atas, melihat fenomena saat ini mengenai perkembangan ilmu pengetahuan dan teknologi telah disalahgunakan sebagai sarana tindak pidana, oleh karena itu menjadi penting

[4] Donny Ariyus, *Computer Security*, Andi Offset, Yogyakarta, 2006, hlm. 2.

untuk merumuskan suatu kebijakan hukum agar pelaku tindak pidana *cybercrime* dapat diminta pertangungjawaban hukum (pidana).

Adanya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi, dapat dibaca sebagai salah satu upaya pemerintah dalam melakukan penegakan hukum pidana sesuai dengan *asas legalitas* (perbuatannya yang dapat dipersalahkan atas dasar peraturan perundang-undangan yang telah ada sebelumnya). Walaupun demikian, harus diakui bahwa persoalan tindak pidana yang terjadi di internet (dunia *cyber*) merupakan suatu delik baru dalam perkembangan hukum pidana. Salah satu tindak pidana dalam dunia maya (*cybercrime*)[5] yang sedang berkembang dan banyak terjadi adalah tindak pidana *hacking* dan *carding*. Salah satu contoh

[5] Kasus tindak pidana *cyber crime* yang pernah terjadi di Indonesia adalah Emilia Karolia. Kronologi kasusnya bermula ketika Emilia Karolia berkenalan, dan menjalin hubungan cinta dengan Dewa Putu Dirga. Namun, sekitar bulan Juli 2004 Emilia Karolia mengetahui bahwa Dewa Putu Dirga telah menjalin hubungan cinta dengan seseorang wanita warga negara Amerika Serikat bernama Kathryn Hopkins, dan telah memutuskan hubungan cintanya dengan Emilia Karolia melalui *e-mail*. Atas dasar peristiwa tersebut, Emilia Karolia merasa dihianati oleh Dewa Putu.

Emilia Karolia meminta penjelasan dari Dewa Putu Dirga melalui *e-mail*, namun jawaban dari Dewa Putu Dirga tidak dapat diterima oleh Emilia Karolia. Sehingga Emilia Karolia mengancam melalui *e-mail* akan menghilangkan nyawa Dewa Putu Dirga, keluarga, dan kekasihnya, serta mengancam menaruh menaruh bom dan akan menghancurkan *Falls Church City Public School* di Virginia USA tempat Kathryn Hopkins bekerja.

Perbuatan tindak pidananya dilakukan bermula ketika tahun 2002, Emilia Karolia melakukan pengancaman melalui e-mail yang dikirimkan dari warnet Sport@Net di Jl. Melawai III No.12 Kebayoran Baru Jakarta Selatan dengan menggunakan user name Abdul Aziz yang beralamat ulovemeilovemeyoukillme@yahoo.com ditujukan ke alamat e-mail server milik *Falls Church City Public School* di Virginia USA yaitu hopkins@fccps.k12.va.us, Confam4@earthlink.net dan beberapa server lainnya di Virginia USA.

Akibat *e-mail* tersebut sekolah dikosongkan, guru-guru disuruh pulang, rapat sekolah dibatalkan, sekolah ditutup, dan tetap di bawah pengawasan polisi, serta anjing pelacak didatangkan untuk melakukan pelacakan. Setelah kejadian tersebut Emilia Karolia ditangkap dan dipejara. Delik yang dituduhkan pada Emilia Karolia adalah tindak pidana pengancaman menghilangkan nyawa Dewa Putu Dirga, keluarga, kekasih, dan pengancaman bom. Kasus tersebut diputus oleh Pengadilan Negeri Jakarta Selatan, dengan hukuman penjara tiga bulan. Dalam Perkara Nomor: Putusan Nomor 2098/Pid.B/2005/PN.JS atas nama terdakwa Emilia Karolia, January 2005.

kasus yang menarik dari tindak pidana tersebut yang pernah terjadi di Indonesia adalah kasus di bawah ini.

Pada tahun 1997, ketika masalah Timor Timur menghangat, situs Departemen Luar Negeri dan ABRI (Angkatan Bersenjata Republik Indonesia) yang sekarang disebut TNI (Tentara Nasional Indonesia) dibobol oleh para *cracker Porto* (Portugis) yang pro-kemerdekaan Timor Timur. *Frontpage* (desain depan atau beranda) kedua situs itu diganti semua. Selain itu, aksi yang disebut *East Timor Campaigne* itu juga menambahkan pada situs yang diserang dengan kata-kata anti-integrasi Timor Timur dan anti ABRI.

Dalam tahun yang sama, situs pendidikan di Indonesia juga ikut dirusak oleh para *cracker* tersebut. Situs yang dirusak adalah situs milik LIPI dan UNAIR (Universitas Airlangga). Dikarenakan serangan para *craker Porto* yang membabi buta tanpa memandang apakah itu situs pendidikan, pemerintah atau bisnis, maka para *cracker* dari Indonesia membalas untuk menyerang Toxin: pangkalan kelompok anti-integrasi di internet.

Yang paling menghebohkan, serangan (balik) itu tidak hanya menghancurkan *homepage* tapi juga menghantam perusahan penyedia server di Irlandia, yaitu Connect Ireland. Perusahaan ini ikut diserang karena dikenal sebagai penyedia server untuk situs yang beroperasi di bawah *East Timorese*

Project, yaitu *web* yang memperjuangkan kemerdekaan Timor Timur untuk lepas dari Indonesia.[6]

Kasus di atas merupakan contoh kecil *cybercrime* yang pernah terjadi di Indonesia. Jika dilihat lebih jauh, secara kuantitas tindak pidana tersebut sangatlah banyak, terutama di kota-kota besar di Indonesia, seperti: Jakarta, Bandung, Surabaya, Semarang, dan DIY (Daerah Istimewa Yogyakarta).

Berangkat dari fenomena itu, penulis akan mencoba meneliti sejauh mana penindakan hukum tindak pidana *cybercrime*, khususnya *hacking* dan *carding* di D.I.Y. DIY dipilih sebagai subjek penelitian karena di samping merupakan kota pelajar, untuk saat ini D.I.Y. merupakan percontohan kota *cyber* di antara kota-kota lainnya di Indonesia. Dengan demikian, dapat diasumsikan bahwa D.I.Y. berpotensi besar sebagai lokasi terjadinya berbagai tindak pidana *cybercrime*.

Berangkat dari latar belakang di atas, penulisan skripsi ini diberi judul sebagai berikut: "**PENEGAKAN HUKUM TERHADAP TINDAK PIDANA *HACKING* DAN *CARDING* DI DAERAH ISTIMEWA YOGYAKARTA."**

B. Permasalahan

Berdasarkan latar belakang di atas maka dapat dirumuskan beberapa rumusan masalah sebagai berikut:

1. Apakah yang melatarbelakangi terjadinya tindak pidana *hacking* dan *carding* di Daerah Istimewa Yogyakarta?

[6] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* Rafika Aditama, Bandung, 2005, hlm. 61.

2. Bagaimana penegakan hukum tindak pidana *hacking* dan *carding* di Daerah Istimewa Yogyakarta?

C. Tujuan Penelitian

Tindak pidana *hacking* dan *carding* adalah tindak pidana yang unik. Disebut unik karena tindak pidana ini menggunakan sarana komputer untuk melakukan tindak pidana. Meskipun demikian, pemerintah dan aparat penegak hukum terus mengupayakan penegakkan hukum agar dapat menekan tindak pidana tersebut.

Sesuai dengan latar belakang di atas penulisan skripsi ini dilakukan untuk:

1. Mengetahui bagaimana tindak pidana *hacking* dan *carding*.
2. Mengetahui bagaimana penegakan hukum tindak pidana *hacking* dan *carding*.

D. Tinjauan Pustaka

Kemajuan berpikir umat manusia telah menciptakan teknologi. Dilihat dari asal katanya, teknologi berasal dari bahasa Yunani yaitu *technologia* yang artinya pembahasan sistematik tentang seluruh seni dan kerajinan *(systematic treatment of the arts and crafts)*. Perkataan tersebut mempunyai akar kata: *techne* (perkataan atau pembicaraan) dan *logos* (ilmu). Akar kata *techne* pada zaman Yunani kuno berarti seni *(art),* kerajinan *(craft).*[7]

[7] Ronny Hanitijo Soemitro, "Hukum dan Perkembangan Ilmu Pengetahuan dan Teknologi di Dalam Masyarakat", Pidato Pengukuhan pada Penerimaan Jabatan Guru Besar Tetap Fakultas Hukum UNDIP, Semarang, 6 Desember 1990, hlm. 8. Diunduh dari: www.google-pidato pengukuhan.com, pada hari Minggu, 24 Juni 2012.

Selain itu, teknologi juga dapat diartikan sebagai *the know-how of making things*, yang secara garis besar mempunyai arti sebagai kemampuan untuk mengerjakan sesuatu dengan hasil nilai yang tinggi, baik nilai kegunaan maupun nilai jual.[8]

Terlepas dari itu, harus diakui bahwa pesatnya perkembangan di bidang teknologi informasi saat ini merupakan dampak dari semakin kompleksnya kebutuhan manusia akan informasi itu sendiri. Dekatnya hubungan antara informasi dan teknologi jaringan komunikasi telah menghasilkan dunia maya yang amat luas yang biasa disebut dengan *cyber space*. Teknologi ini berisikan kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan komputer yang disebut jaringan internet.[9]

Internet merupakan teknologi yang sudah mendunia dan memasyarakat bagi semua kalangan. Melalui jaringan internet, pengguna dapat mengakses apa pun setiap saat.[10] Sebagai media penyedia informasi, internet merupakan sarana kegiatan komunitas terbesar dan terpesat pertumbuhannya.[11]

Pesatnya pertumbuhan internet ini memungkinkan terjadinya tindak pidana serta penyimpangan-penyimpangan yang dilakukan para penggunanya

---

[8] Marsetio Donoseputro, "Pendidikan, Iptek dan Pembangunan", dimuat di harian: Surabaya Post, Kamis, 20 Maret 1991.

[9] Teguh Arifiyadi, "Tantangan Bagi Perkembangan Hukum di Indonesia, *Cyber Law",* diunduh dari: http://inikan.wordpress.com/2008/03/27/*cyberlaw-tantangan-bagi-perkembangan-hukum-di-indonesia*, pada tanggal 24 Juni 2012.

[10] Abdul Wahid dan Mohammad Labib, Op. cit, hlm. 24.

[11] Fajriyanto, "Internet dalam Tinjauan Agama dan Teknologi", makalah pada Seminar Problematika Pornografi Pada Media Internet, Yogyakarta, 2007, hlm. 5.

di dunia maya sehingga menimbulkan dampak negatif bagi kemajuan manusia dan jaringan *network* di internet itu sendiri. Pelaku tindak pidana ini tidak hanya berasal dari satu daerah atau negara saja, melainkan sudah hampir setiap negara terdapat pelaku tindak pidana di bidang teknologi informasi.

Indra Safitri mengemukakan bahwa tindak pidana dunia maya adalah jenis tindak pidana yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas yang memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[12]

Tindak pidana di bidang teknologi informasi sering disebut juga dengan *cybercrime*. Tindak pidana ini dilakukan di internet dengan menggunakan *software* yang kemudian terinstal di aplikasi *windows*, serta dikoneksikan ke jaringan *network* di *internet*. Dengan adanya *cybercrime* tersebut maka diperlukan suatu perangkat hukum untuk melindungi korban, menegakkan keadilan guna memberi efek jera bagi pelaku tindak pidana.

Hukum dapat diartikan sebagai sekumpulan aturan atau seperangkat norma yang dibentuk oleh lembaga formal dengan tujuan untuk mengatur masyarakat, yang apabila dilanggar mengakibatkan sanksi.[13]

---

[12] Indra Safitri, "Tindak Pidana di Dunia Cyber," dalam Insider, Legal Journal From Indonesian Capital & Investmen Market, diunduh dari: http://business.fortunecity.com/buffett/842/art180199_*tindakpidana*.htm, pada tanggal 24 Juni 2012.

[13] Anton F. Susanto, *Hukum (Dari Consilience Menuju Paradigma Hukum Konstruktif-Transgresif)*, Rafika Aditama, Bandung, 2007, hlm. 9.

Esmi Warassih Pujirahayu menjelaskan bahwa hukum merupakan *the normative life of the state and its citizens*; hukum menentukan serta mengatur bagaimana hubungan itu dilakukan dan bagaimana pula akibatnya. Hukum memberikan pedoman tingkah laku, baik tingkah laku yang dilarang, dibutuhkan, maupun diizinkan. Penormaan ini dilakukan dengan membuat kerangka umum dan kemudian dijabarkan lebih lanjut dalam berbagai bentuk peraturan perundang-undangan yang ada.[14]

Hukum mengenal adanya kaedah hukum yang ditujukan terutama kepada pelakunya yang konkrit, yaitu pelaku pelanggaran yang nyata-nyata berbuat, bukan untuk penyempurnaan manusia melainkan untuk ketertiban masyarakat agar masyarakat tertib agar jangan sampai jatuh korban agar tidak terjadi tindak pidana.[15]

Timbulnya hukum sekurang-kurangnya harus ada kontak antara dua orang. Tetapi pada hakekatnya hukum baru ada, baru dipersoalkan, apabila ada konflik kepentingan. Konflik kepentingan ini terjadi apabila dalam melaksanakan kepentingan atau memenuhi kebutuhan manusia merugikan orang lain.[16]

Konflik kepentingan di dunia maya, otomatis ada yang dirugikan dan ada yang mendapatkan keuntungan. Di dunia maya yang dirugikan adalah korban *cybercrime,* sedangkan yang mendapat keuntungan di sini adalah

[14] Esmi Warassih P, *Pranata Hukum (Sebuah Telaah Sosiologis),* Suryandaru Utama, Semarang, 2005, hlm. 36.
[15] Sudikno Mertokusumo, *Mengenal Hukum-Suatu Pengantar*, Liberty, Yogyakarta, 2005, hlm. 12.
[16] *Ibid*., hlm. 30-31.

pelaku tindak pidana *cybercrime*. Untuk meminimalisir konflik kepentingan di dunia maya maka diperlukan penegakan hukum.

Berbicara mengenai penegakan hukum terhadap tindak pidana *cybercrime* berarti menganalisa tindak pidana *cybercrime*, yaitu modus operandi tindak pidana *hacking* dan *carding*.

Dalam hukum pidana, bahwa suatu tindak pidana dapat digolongkan sebagai suatu perbuatan itu jika masuk ke dalam ruang lingkup pidana. Hukum pidana materiil mempunyai ruang lingkup pada apa yang disebut "tindak pidana" atau *"strefbaar feit."*[17]

Tindak pidana *cybercrime* di dalam buku *cybercrime* (modus operandi dan penanggulangan) adalah tindak pidana yang dilakukan oleh seseorang maupun kelompok dengan menggunakan sarana komputer dan alat komunikasi lainnya. Sedangkan *cyberspace* adalah ruang maya terhubungnya komputer dengan saluran penyedia jasa internet yang dapat diakses kapan saja, tidak mengenal batas ruang dan waktu.[18]

Menurut kepolisian Inggris, *cybercrime* dapat diberi pengertian sebagai segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Dalam definisi tersebut tidak dijelaskan apa yang dimaksud

---

[17] Adami Chazawi, *Pelajaran Hukum Pidana I*, cetakan Kedua, Rajawali Pers, Jakarta, 2005, hlm. 67.

[18] H. Sutarman, *Cyber Crime (Modus Operandi dan Penanggulangannya)*, LaksBang PRESSindo, Yogyakarta, 2007, hlm. 4.

dengan arti kata jaringan komputer. Apabila dimaknai secara luas maka akan meliputi LAN dan internet.[19]

Tindak pidana komputer atau *cybercrime* adalah upaya memasuki atau menggunakan fasilitas komputer atau jaringan komputer tanpa seijin dan dengan melawan hukum dengan atau tanpa menyebabkan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.[20] Tindak pidana *hacking* dan *carding* termasuk tindak pidana *cybercrime*. Pelaku tindak pidana *hacking* disebut juga *hacker*, adalah orang yang memasuki atau mengakses jaringan komputer secara tidak sah (tanpa ijin) dengan suatu alat dan program tertentu, yang bertujuan untuk merusak dan merubah data dengan menambah atau mengurangi.[21]

Berbeda dengan tindak pidana *carding*, pelaku tindak pidana *carding* disebut *carder*, yaitu orang yang memalsukan nomor kartu kredit orang lain untuk bisa mendatangkan berbagai produk komersial yang diperjualbelikan lewat internet.[22]

Tindak pidana *hacking* dan *carding* adalah modus operandi baru dalam dunia hukum, sehingga memerlukan penegakan hukum yang serius agar dapat menekan modus operandi tindak pidana *cybercrime* lainnya demi terciptanya keamanan serta keadilan bagi masyarakat.

---

[19] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* Rafika Aditama, Bandung, 2005, hlm. 40.
LAN ini mempunyai karakter yang berbeda dengan internet. LAN merupakan jaringan yang tertutup karena dalam kategori tertentu tindak pidana *cybercrime* tidak dapat dilakukan.

[20] Didik M. Arif Mansur dan Elasatris Gultom, *Cyber law (Aspek Hukum Teknologi Informasi)*, Refika Aditama, Bandung, 2005, hlm. 8.

[21] H. Sutarman, *Cyber Crime (Modus Operandi dan Penanggulangannya)*, LaksBang PRESSindo, Yogyakarta, 2007, hlm. 68.

[22] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* Rafika Aditama, Bandung, 2005, hlm. 130.

Penegakan hukum adalah rangkaian proses untuk menjabarkan nilai, ide, cita yang cukup abstrak yang menjadi tujuan hukum. Tujuan hukum atau cita-cita hukum memuat nilai-nilai moral, seperti keadilan dan kebenaran. Nilai-nilai tersebut harus mampu diwujudkan dalam realitas nyata. Eksistensi hukum diakui apabila nilai-nilai moral yang terkandung dalam hukum tersebut mampu diimplementasikan atau tidak.[23]

Soerjono Soekanto mengatakan, bahwa secara konseptual, inti dan arti penegakan hukum terletak pada kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan di dalam kaidah-kaidah yang mantap dan mengejewantah sikap tindak tersebut sebagai rangkaian penjabaran nilai tahap akhir untuk menciptakan, memelihara, dan mempertahankan kedamaian pergaulan hidup.[24]

Hukum pidana sudah jelas konsekuensinya, itu terlihat jika melanggar aturan-aturan atau larangan yang telah dibuat sebelumnya harus mendapatkan sanksi pidana. Namun dalam penegakan hukumnya harus sesuai prosedur, karena pada dasarnya perbuatan seseorang harus diadili sesuai dengan *lex temporis delicti* (aturan yang berlaku pada saat tindak pidana dilakukan).[25] Hal inilah yang menyulitkan aparat penegak hukum dalam melakukan penegakan hukum pidana.

Multi tafsirnya peraturan yang ada saat ini dalam mengatur *cybercrime* maupun tindak pidana pada umumnya, menjadi suatu hambatan

---

[23] Satjipto Rahardjo, *Penegakan Hukum (Suatu Tinjauan Sosiologis)*, Genta Publishing, Yogyakarta, 2009, hlm. vii.
[24] *Ibid.*
[25] Yeni Widowaty, dan Mukhtar Zuhdy dan Trisno Raharjo dan M. Endrio Susila, *Hukum Pidana*, Lab. Hukum, Yogyakarta, 2009**,** hlm. 12.

tersendiri bagi aparat penegak hukum. Sedangkan di dalam hukum pidana dan peraturan yang ada, dapat berlaku surut, yaitu pengecualian jika dalam hal ada perubahan perundang-undangan setelah perbuatan dilakukan.

Penegak hukum wajib kiranya untuk menyebarluaskan informasi kepada masyarakat, bahwa *cybercrime* adalah suatu tindak pidana yang dapat dijatuhi hukuman kepada pelakunya dan sekiranya perlu melakukan sosialisasi kepada masyarakat luas akan bahaya yang ditimbulkan *cybercrime*.

E. Metode Penelitian

Dalam melakukan penelitian, penulis menggunakan metode penelitian sebagai berikut :

1. Jenis Penelitian

   Penulisan skripsi ini jenis penelitian yang digunakan adalah penelitian yuridis normatif. Penelitian yuridis normatif adalah penelitian yang dilakukan dengan cara mengkaji dan menganalisa data sekunder yang berupa bahan hukum primer, sekunder, dan tersier. Penulis akan meneliti fakta-fakta yuridis sebagai batasan normatif bagi penegakkan hukum tindak pidana *hacking* dan *carding*. Selanjutnya, penulis akan meneliti fakta-fakta di lapangan serta kepustakaan untuk kemudian dapat dianalisis berdasarkan ketentuan-ketentuan normatif yang berlaku.

2. Lokasi Penelitian

   Sesuai dengan judul skripsi ini penelitian dilakukan di Daerah Istimewa Yogyakarta, di berbagai institusi dengan lokasi sampel sebagai berikut;

a. Wilayah Kota dengan instansi yaitu Pengadilan Negeri Yogyakarta, Polresta Yogyakarta.
b. Wilayah Sleman dengan instansi yaitu Pengadilan Negeri Sleman, Polda Daerah Istimewa Yogyakarta.

3. Sumber Data

Sumber data yang dibutuhkan dalam penelitian ini terbagi atas dua kategori, yaitu:

a. Data Primer yaitu data yang diperoleh secara langsung dari hasil penelitian lapangan melalui wawancara langsung kepada narasumber, yaitu: Bapak Wahyu Asmiadi.
b. Data Sekunder yaitu data yang diperoleh melalui studi kepustakaan, mempelajari literatur, dokumen resmi, peraturan perundang-undangan, maupun yang berkaitan dengan obyek atau permasalahan dalam penelitian. Bahan-bahan hukum yang dapat dijadikan obyek studi kepustakaan meliputi bahan hukum primer dan bahan hukum sekunder:
    1) Bahan hukum primer adalah peraturan perundang-undangan dan dokumen resmi yang berhubungan erat dengan permasalahan yang diteliti. Bahan hukum primer dalam penelitian ini bersumber dari:
        a) Undang-Undang Dasar Tahun 1945.
        b) Kitab Undang-Undang Hukum Pidana.
        c) Undang-undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana.

d) Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

e) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2) Bahan hukum sekunder adalah bahan-bahan hukum yang memberikan penjelasan mengenai bahan hukum primer. Bahan hukum sekunder dalam penelitian ini bersumber dari:

a) Literatur-literatur hukum pidana dari berbagai pengarang.

b) Makalah, jurnal, surat kabar, media electronik, dokumen, tulisan ilmiah, dan artikel-artikel yang mempunyai relevansi dengan masalah kejahatan *hacking* dan *carding*.

3) Bahan hukum tersier yaitu bahan hukum yang menjelaskan tentang bahan hukum primer dan bahan hukum sekunder, yang terdiri dari:

a) Kamus Hukum.

b) Kamus Istilah Internet.

4. Narasumber Penelitian

Untuk mendukung keakuratan data maka dilakukan wawancara dengan narasumber yang dapat memberikan keterangan mengenai data yang dibutuhkan dalam penelitian yang berkaitan dengan tindak pidana *hacking* dan *carding*. Narasumber tersebut yaitu: Bapak Wahyu Asmiadi.

5. Metode Pengumpulan Data

Pengumpulan data dilakukan dengan cara studi pustaka, yaitu kegiatan meneliti atau menggali bahan-bahan hukum atau data tertulis,

baik yang berupa peraturan perundang-undangan, buku-buku, majalah-majalah, jurnal-jurnal hasil penelitian, serta bahan-bahan tertulis yang berhubungan atau berkaitan dengan tindak pidana *hacking* dan *carding*.

6. Analisis Data

Dalam melakukan penyajian terhadap data yang diperoleh, penulis menggunakan teknik penyajian deskriptif kualitatif. Data yang diperoleh akan dijelaskan, dipilih, dan diolah berdasarkan kualitasnya yang relevan dengan tujuan dan masalah yang akan diteliti dalam hal ini masalah tindak pidana *hacking* dan *carding*.

F. Sistematika Penulisan Skripsi

Penulisan skripsi ditulis dalam 5 (lima) Bab, yang terdiri atas: Pendahuluan, Tinjauan Umum Tindak Pidana *Hacking* dan *Carding*, Penegakan Hukum Dalam Tindak Pidana *Hacking* dan *Carding*, Hasil Penelitian dan Analisis Penegakan Hukum di Daerah Istimewa Yogyakarta, dan Penutup. Berikut adalah uraian singkat masing-masing bab:

1. Bab I tentang Pendahuluan. Bab ini berisi mengenai latar belakang, permasalahan, tujuan penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.
2. Bab II tentang Tinjauan Umum Tindak Pidana *Hacking* dan *Carding*. Bab ini berisi mengenai pengertian tindak pidana *cybercrime*, macam-macam tindak pidana *cybercrime*, pengertian *hacking* dan *carding*, peraturan-peraturan yang mengatur tindak pidana *hacking dan carding.*

3. Bab III tentang Penegakan Hukum dalam Tindak Pidana *Hacking* dan *Carding*. Bab ini berisi pengertian penegakan hukum, peran dan fungsi penegak hukum.
4. Bab IV tentang Hasil Penelitian, Analisi dan Pembahasan Penegakan Hukum. Bab ini menjelaskan faktor-faktor yang melatarbelakangi tindak pidana *hacking* dan *carding* di Daerah Istimewa Yogyakarta serta penegakan hukumnya di Daerah Istimewa Yogyakarta.
5. Bab V tentang Penutup. Bab ini memberi kesimpulan dan saran serta lampiran tentang penelitian yang telah dilakukan.