

BAB 1

PENDAHULUAN

A. Latar Belakang Penelitian

Dewasa ini, lembaga perbankan menjadi salah satu tumpuan harapan dalam menggerakkan roda perekonomian nasional khususnya sektor riil. Hasil dari kebijakan deregulasi sektor perbankan pada tahun 1990-an telah menyebabkan tumbuh suburnya bank-bank bak cendawan dimusim hujan. Booming bank-bank tersebut ternyata tidak di iringi dengan ketahanan modal usaha perbankan. Selain itu, pengawasan Bank Indonesia yang lemah terhadap bank-bank dan praktik kejahatan perbankan yang terus meningkat kuantitas dan kualitasnya dari waktu ke waktu, turut andil melemahkan lembaga perbankan. Salah satu penyebabnya adalah munculnya berbagai kejahatan perbankan yang bersifat nasional maupun internasional. Kejahatan yang dikategorikan sebagai kejahatan kerah putih (*whitecollar crime*).

Kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dengan Internet dalam segala bidang seperti e-banking, ecommerce, e-government, e-education dan banyak lagi telah menjadi sesuatu yang lumrah. Bahkan apabila masyarakat terutama yang hidup di kota besar tidak bersentuhan dengan persoalan teknologi informasi dapat dipandang terbelakang atau "GAPTEK". Internet telah menciptakan dunia baru yang

dinamakan cyberspace yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk virtual (tidak langsung dan tidak nyata). Walaupun dilakukan secara virtual, kita dapat merasa seolah-olah ada di tempat tersebut dan melakukan hal-hal yang dilakukan secara nyata, misalnya bertransaksi, berdiskusi dan banyak lagi.

Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif kita semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi ini, misalnya kita dapat melakukan transaksi perbankan kapan saja dengan e-banking, e-commerce juga membuat kita mudah melakukan pembelian maupun penjualan suatu barang tanpa mengenal tempat. Mencari referensi atau informasi mengenai ilmu pengetahuan juga bukan hal yang sulit dengan adanya e-library dan banyak lagi kemudahan yang didapatkan dengan perkembangan Internet. Tentunya, tidak dapat dipungkiri bahwa teknologi Internet membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat dilakukan dengan menggunakan media komputer secara online dengan risiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara disamping menimbulkan kejahatan-kejahatan baru.

Kejahatan perbankan tidak hanya dilakukan oleh pihak-pihak di luar perbankan, tetapi juga melibatkan pihak-pihak di lingkungan perbankan sendiri. Banyak modus operandi yang dilakukan dalam kejahatan ini, salah satunya pada usaha kartu kredit.

Mencermati hal tersebut dapatlah disepakati bahwa kejahatan IT/Cybercrime memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar KUHP. Perkembangan teknologi informasi yang demikian pesatnya haruslah diantisipasi dengan hukum yang mengaturnya dimana kepolisian merupakan lembaga aparat penegak hukum yang memegang peranan penting didalam penegakan hukum, sebab tanpa adanya hukum yang mengatur dan lembaga yang menegakkan maka dapat menimbulkan kekacauan didalam perkembangannya.

Seiring dengan meningkatnya penggunaan kartu kredit di Indonesia, tingkat risiko kredit yang disebabkan memburuknya tingkat kolektibilitas dan potensi meningkatnya kriminalitas seperti pemalsuan kartu kredit dengan berbagai modus operandinya juga naik cukup tajam. Menurut data dari Asosiasi Kartu Kredit Indonesia (AKKI) pada Juli 2003- April 2006 mencapai Rp 41.000.000.000 (empat puluh satu miliar). Nilai kerugian ini cukup tinggi jika dibandingkan dengan jumlah kasus yang masuk selama periode itu yang hanya 89 kasus. Itu artinya per kasus nilai kerugian Rp4,600.000.000 (empat miliar enam ratus juta). Jakarta masih menjadi

daerah operasi terbesar kejahatan kartu kredit dengan 54 kasus, lalu disusul Surabaya 9 kasus, Denpasar 6 kasus dan sisanya kota-kota besar lain.¹

Pada umumnya modus operandi kejahatan kartu kredit lebih condong karena proses seleksi aplikasi calon pemegang kartu kredit yang kurang teliti, sehingga kartu kredit jatuh kepada orang yang tidak bertanggung-jawab sehingga melakukan kejahatan pemakaian kartu.² Selain itu, kasus menonjol lainnya adalah pelaku kejahatan mengaku dari penerbit kartu kredit dan menelepon pemegang kartu serta menanyakan nomor kartu yang lalu dipakai untuk transaksi ilegal. Praktik kejahatan kartu kredit yang tergolong canggih ditemukan pada kasus-kasus counterfeiting (pemalsuan). Pada kasus ini, pelaku kejahatan memakai alat tertentu yang dapat melakukan penyalinan informasi yang ada pada kartu. Umumnya hal ini terjadi pada kartu kredit berbasis magneticstripe yang merupakan jenis kartu id card yang mampu menyimpan data dengan memodifikasi magnet yang kecil berbasis besi partikel magnetik pada pita bahan kartu magnetik yang digesekkan pada alat tertentu yang berfungsi seperti electronic data capturing (EDC). EDC merupakan mesin yang berfungsi sebagai sarana penyedia transaksi dan alat pembayaran yang penggunaannya dengan cara memasukkan atau menggesek kartu ATM, kartu debit maupun kartu kredit dilengkapi dengan fasilitas pembayaran lainnya yang terkoneksi secara realtime. Sedapat mungkin pemegang kartu kredit jangan memberi kesempatan pelaku kejahatan

¹ Data diakses dari <http://www.bi.go.id/web/id/SP001/Info01/DASP01/info-fraud.htm>, Portal Bank Indonesia, *Kerugian Card Fraud Masih Cukup Tinggi*, tanggal 30 Juli 2007, pukul 19.00 WIB.

² *Ibid*

menggesekkan kartu pada alat skimmingnya. Sedangkan modus kejahatan wire tapping (kawat penyadap), si pelaku melakukan penyadapan informasi melalui jaringan telepon, PABX atau LAN yang terhubung dengan jaringan EDC.

Adapun modus operandi kejahatan kartu kredit terus berkembang dari waktu ke waktu. Sekitar 15 tahun yang lalu, kejahatan kartu kredit hanya dilakukan melalui pencurian kartu kredit, lalu dipalsukan tanda tangannya. Setelah pihak bank mengeluarkan kartu yang mempunyai foto, nomor kartu kredit lalu diratakan dengan suatu alat cetak ulang. Modus operandi kemudian berkembang dengan menggunakan metode penggandaan sebuah alat sehingga data kartu kredit bisa dipindahkan ke kartu palsu sehingga batas kartu kredit asli itu sudah ada di kartu kredit palsu. Alat penggandaan tersebut dijual bebas di pasaran. Modus ini berkembang lagi, dengan melakukan penanaman kartu chip dalam mesin elektronik data yang ada di toko-toko. Modusnya, pelaku tindak pidana berpura-pura sebagai anggota bank untuk memeriksa alat itu, meletakkan chip selama beberapa waktu, setelah itu mengambil chip dan memindahkan ke kartu kredit palsu. Modus operandi terakhir adalah penyadapan jalur telekomunikasi.³

Di Balikpapan, Kalimantan Timur, Mudi Koestiwa bukan satu-satunya orang yang diduga menggunakan kartu kredit palsu. Hanya dalam waktu dua bulan, sudah tiga orang yang ditahan petugas Polres Kota Balikpapan karena tuduhan menggunakan kartu kredit palsu, yakni Veranita (30), Benny Wong

³ Data di akses dari <http://www.kompas.com/> *Pemalsuan Kartu Kredit Semakin Merajalela*, tanggal 31 Juli 2007, pukul 20.00 WIB.

(35) yang kini penahanannya ditangguhkan, serta Mudi Koestiwa (38) yang kasusnya sedang diproses di pengadilan. Modus yang dilakukan oleh tiga orang ini semuanya sama, yakni menggunakan kartu kredit yang seluruhnya palsu dan bukan kartu asli hasil curian. Baik fisik kartu, logo serta hologram semuanya palsu. Namun, data nama dan nomor pemegang kartu benar-benar ada dan masih berlaku (valid). Karena itu, ada dugaan kuat ketiga pelaku merupakan bagian dari sindikat internasional pemalsu kartu kredit.

Pengadilan Negeri Gianyar, Bali pada 6 Juni 2005 menjatuhkan putusan pidana 2,8 tahun atas Beny Wong seorang terdakwa pemalsu kartu kredit. Seperti sebelumnya terdakwa yang sama sudah mendapatkan hukuman tiga tahun oleh Pengadilan Negeri Denpasar pada 14 September 2004. Sehingga, secara keseluruhan pemalsu kartu kredit ini harus mendekam selama 5 tahun 8 bulan merupakan putusan tertinggi dalam sejarah kartu kredit di Indonesia sejak industri itu diperkenalkan pertama kali di Tanah Air sekitar 1985.⁴

Para pemalsu kartu kredit mempunyai mesin pembuat kartu. Mesin *encoding* kartu ini sering dipakai untuk membuat tanda pengenal atau ID Card, kartu anggota, dan sebagainya. Bahan kartu dibeli dari luar negeri, atau dari bank di dalam negeri kemudian dicetak sesuai dengan tampilan aslinya. Dicitaknya nama pemilik pada kartu (*embossing*) dan *encoding* data pada magnetic stripe kartu sesuai dengan data yang terekam pada kartu asli. Data dan nomor awalnya didapat dengan cara *skimming*, yaitu: merekam secara

⁴ Data diakses dari <http://www.bisnis.com/servlet/page?-pageid=483&-dad=portal30&-schema=PORTAL30&pared-id=368336>, ***Kejahatan Kartu Kredit Diganjar Setimpal***, tanggal 1 Agustus 2007, pukul 16.49 WIB.

elektronik data pada *magnetic stripe*, *skimming* ini biasanya dikerjakan dengan suatu alat sebesar kotak korek api atau kotak kartu poker yang dititipkan oleh pelaku yang akan mencuri data dan nomor dari kartu kredit asli pada restoran, hotel, toko, tempat-tempat yang biasa melakukan pembayaran misalnya pada kasir, kartu setelah digesek pada kasir pembayaran digesek ulang pada alat tersebut yang disembunyikan dibawah meja yang langsung oleh *skimmer* tersebut direkam tanpa sepengetahuan pemilik kartu.

Dalam usaha kartu kredit terdapat berbagai masalah yang dapat merugikan usaha kartu kredit, yang pada akhirnya kerugian harus ditanggung oleh bank atau nasabah pemegang kartu kredit (*card holder*). Kerugian ini disebabkan adanya kejahatan kartu kredit yang semakin modern dan mempunyai jaringan luas, jaringan ini telah sampai ke luar negeri baik dari segi teknik maupun peralatan dan bahan baku pembuat kartu kredit palsu, jaringan ini telah saling menginformasikan dan saling jual beli bahan-bahan baku untuk pemalsuan.

Pemilik *skimming* bisa orang lain yang menitipkan pada karyawan atau kasir, tapi bisa juga karyawannya sendiri yang kemudian dijual pada jaringan pembeli data dan nomor kartu kredit. Cara lain dari pencurian data dan nomor pemilik kartu kredit asli ini, yaitu dengan memasang semacam chip pada terminal POS (*Point of Sale*) yaitu: alat gesek kartu kredit yang digunakan untuk pembayaran pada toko, restoran, atau hotel, pelaku disini bisa petugas service terminal POS, karyawan pada terminal POS, atau orang

lain yang menipiskan. Tetapi umumnya chip ini harus dipasang oleh petugas yang menangani terminal POS, misalnya pada saat service dan sebulan kemudian chip itu telah penuh dengan data di ambil lagi, dengan cara *skimming* dan *chip informasi card verification value (CVV)* yang memiliki tiga digit angka yang berfungsi sebagai pengamanan kartu kredit ikut terekam.⁵

Menyadari banyaknya laporan kejahatan kartu (card fraud) di masyarakat, Bank Indonesia menerbitkan aturan yang mewajibkan bank meningkatkan fitur keamanan pada kartu yang diedarkan. Salah satu fitur yang disarankan Bank Sentral adalah memakai teknologi chip. Diharapkan dengan pemakaian chip, keamanan pemakai kartu dapat semakin terjaga. Hal ini disebabkan karena teknologi chip memuat sejumlah aplikasi dan pengamanan yang berlapis berbasis kriptogram.

Upaya pemberantasan kejahatan kartu kredit tentu saja tidak cukup, masih banyak yang harus dibenahi di industri kartu kredit. Sebagai akibat tingginya tingkat kejahatan penyalahgunaan kartu kredit, Kementerian Komunikasi dan Informasi bersama Bank Indonesia sudah menyiapkan draf Rancangan Undang-Undang (RUU) Informasi dan Transaksi Elektronik (ITE) untuk diajukan ke DPR dalam waktu dekat. Deputi Gubernur BI Maulana Ibrahim mengatakan "draf RUU Informasi dan Transaksi Elektronik tersebut antara lain berisi pengaturan tindak pidana dan sanksi pidana dalam kejahatan di transaksi elektronik, termasuk kartu kredit".

⁵ Tb. Irman, *Anatomi Kejahatan Perbankan*, Penerbit PT. MQS Publishing, Bandung, 2006, hlm 154-164

Dengan keluarnya ketentuan ini, diharapkan penanggulangan kejahatan kartu kredit dapat dilakukan secara lebih optimal karena tidak ada lagi kerancuan tentang pasal-pasal hukum yang dapat diterapkan terhadap pelaku tindak kejahatan kartu kredit. Peraturan legal formal yang ada belum mampu mengakomodasi kejahatan kartu kredit, sehingga aspek pengenaan sanksi hukum pelaku kejahatan mengalami kendala dalam pembuktian di lapangan yang terkadang tidak meninggalkan jejak.

Saat ini Indonesia belum memiliki undang-undang yang mengatur *cyber crime*, walaupun undang-undang tersebut sudah ada sejak tahun 2000 namun belum disahkan oleh pemerintah dalam upaya menangani kasus-kasus yang terjadi khususnya yang ada kaitannya dengan *cyber crime*. Sebelum lahirnya undang-undang No. 11 tentang informasi dan transaksi elektronika (ITE), para penyidik (khususnya Polri) menggunakan pasal-pasal di dalam KUHP seperti pasal pencurian, pemalsuan dan penipuan para carder, hal ini jelas menimbulkan berbagai kesulitan dalam pembuktiannya karena mengingat karakteristik dari *cyber crime* sebagaimana telah disebutkan.

Pasal UU ITE yang menjerat kasus penyalahgunaan kartu kredit :

Dalam UU ITE, kasus carding dapat dijerat dengan menggunakan pasal 31 ayat (1) dan pasal 31 ayat (2) yang membahas tentang hacking. Karena dalam salah satu langkah untuk mendapatkan nomor kartu kredit pelaku (carder) sering melakukan hacking ke situs-situs resmi lembaga penyedia kartu kredit untuk menembus sistem pengamannya dan mencuri nomor-nomor kartu kredit tersebut.

Pasal 31 ayat (1): "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronika dan atau dokumen elektronik dalam suatu komputer dan atau sistem elektronik secara tertentu milik orang lain."

Pasal 31 ayat (2): "Setiap orang dengan sengaja atau tanpa hak atau melawan hukum melakukan intersepsi atau transmisi elektronik dan atau dokumen elektronik yang tidak bersifat publik dari, ke dan di dalam suatu komputer dan atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan, penghilangan dan atau penghentian informasi elektronik dan atau dokumen elektronik yang ditransmisikan.

Berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) penyalahgunaan kartu kredit (carding) termasuk dalam Pasal 362 KUHP, dan Pasal 378 KUHP yang merumuskan tentang tindakan pencurian, pemalsuan dan penipuan. Berikut bunyi dan hukuman dalam pasal-pasal tersebut :

Pasal 362 KUHP "Barang siapa mengambil suatu benda yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum". Hukuman : Pidana penjara paling lama 5 tahun atau denda paling banyak sembilan ratus ribu rupiah.

Pasal 378 KUHP "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain dengan melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohongan menggerakkan orang lain untuk menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun

menghapuskan piutang.” Hukuman : Diancam karena penipuan dengan pidana penjara paling lama 4 tahun.⁶

Ada beberapa metode yang biasa digunakan pelaku carding :

1. Hack (*Hacking*)

Pembajakan metode ini dilakukan dengan membobol sebuah website toko yang memiliki system pengamanan yang lemah. Seorang hecker akan meng-hacker suatu website toko, untuk kemudian mengambil data pelanggannya. Carding dengan metode ini selain merugikan pengguna kartu kredit juga akan merugikan toko tersebut karena image-nya akan rusak, sehingga pelanggan akan memilih berbelanja di tempat lain yang lebih aman.

2. Extrapolasi

Seperti yang diketahui, 16 digit nomor kartu kredit memiliki pola algoritma tertentu. Extrapolasi dilakukan pada sebuah kartu kredit yang biasa disebut sebagai kartu master, sehingga dapat diperoleh nomor kartu kredit lain yang nantinya digunakan untuk bertransaksi.

3. Sapu Tangan (*Sniffer*)

Metode ini dilakukan dengan merekam transaksi yang dilakukan oleh seorang pengguna kartu kredit dengan menggunakan software. Hal ini bisa dilakukan hanya dalam satu jaringan yang sama, seperti di warnet atau hostpot area. Pelaku menggunakan software sniffer untuk menyadap transaksi yang dilakukan seorang yang berbeda di satu jaringan yang sama, sehingga pelaku akan memperoleh semua data yang diperlukan untuk selanjutnya

⁶ <http://www.adln.unair.ac.id/go.php?id=jiptunair-gdl-s1-2006-kurniawan13325&PHPSESSID=735f99a341908093de...27k>, **Penegakan Hukum Tindak Pidana Kartu Kredit**, tanggal 22 Agustus 2007, pukul 15.36 WIB

melakukan carding. Pencegahan metode ini adalah website e-commerce akan menerapkan system SSL (Secure Socket Layer) yang berfungsi mengkodekan database dari pelanggan.

4. Phising

Pelaku carding akan mengirim e-mail secara acak dan massal atas nama instansi seperti bank, toko, atau penyedia layanan jasa yang berisikan pemberitahuan dan ajakan untuk login ke situs instansi tersebut. Namun situs yang diberitahukan bukanlah situs asli, melainkan situs yang dibuat sangat mirip dengan situs aslinya. Selanjutnya korban bisa diminta mengisi database disitus tersebut. Metode ini adalah metode paling berbahaya, karena pembajak dapat mendapatkan informasi lengkap dari pengguna kartu kredit itu sendiri. Informasi yang didapat tidak hanya nama pengguna dan nomor kartu kreditnya, namun juga tanggal lahir, nomor identitas, tanggal kadaluarsa kartu kredit bahkan tinggi dan berat badan jika pelaku carding menginginkannya.

Solusi yang dapat dilakukan terhadap carding

1. Pencegahan Dengan Hukum Hukum cyber sangat identik dengan dunia maya, yaitu sesuatu yang tidak terlihat dan semu. Hal ini dapat menimbulkan kesulitan bagi para penegak hukum terkait dengan pembuktian dan penegakan hukum atas kejahatan dunia maya. Selain itu objek hukum cyber adalah data elektronik yang sangat rentan untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Oleh karena itu, kegiatan cyber meskipun bersifat

virtual dan maya dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata.

2. Pencegahan Dengan Teknologi *Handphone* dapat dikatakan merupakan keamanan yang privacy bagi penggunanya. Sms bisa dijadikan sebagai otentikasi untuk mencegah para carding menggunakan kartu kredit illegal. Untuk itu di perlukan suatu proses yang dapat memberikan pembuktian bahwa dengan cara otentikasi melalui sms maka kejahatan carding dapat ditekan sekecil mungkin. Otentikasi sms dapat dilakukan dengan menggunakan tanda
3. Pencegahan Melalui Web Security Penggunaan sistem keamanan web sebaiknya menggunakan keamanan SSL. Untuk data yang disimpan kedalam database sebaiknya menggunakan enkripsi dengan metode algoritma modern, sehingga cryptanalysis tidak bisa mendekripsikannya.
4. Pengamanan Pribadi Pengamanan pribadi adalah pengamanan dari sisi pemakai kartu kredit dan bisa dilakukan dengan cara online maupun *offline*.

Secara *Offline* mungkin anda bisa melakukan hal-hal sebagai berikut:

- a. pastikan kartu kredit yang anda miliki tersimpan pada tempat yang aman.
- b. Jika kehilangan kartu kredit dan kartu identitas anda, segeralah lapor ke pihak berwajib dan segera lakukan pemblokiran pada saat itu juga. Jangan tunggu waktu hingga anda kebobolan karena digunakan oleh orang lain (baik untuk belanja secara offline maupun secara online).

c. Pastikan jika Anda melakukan fotocopy kartu kredit dan kartu identitas tidak sampai digandakan oleh petugas atau pegawai fotocopy. Jangan asal atau sembarang menyuruh orang lain untuk memfotocopykan kartu kredit dan kartu identitas. Secara Online, Anda dapat memperhatikan hal-hal berikut :

- Belanja di tempat yang aman, jangan asal belanja tapi tidak jelas pengelolanya atau mungkin anda baru pertama mengenalnya sehingga kredibilitasnya masih meragukan.
- Pastikan pengelola Web menggunakan SSL (Secure Sockets Layer) yang ditandai dengan HTTPS pada Web Login Transaksi online.

Pendapat Kelompok Mengenai Kasus dan Hukumannya :

Carding adalah kejahatan dengan menggunakan teknologi computer melalui jaringan internet untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil, juga sebagai perbuatan melanggar hukum. Dan dapat diartikan sebagai penipuan kartu kredit online. Jadi bagi pengguna kartu kredit yang sering melakukan belanja atau bertransaksi dalam dunia maya disarankan lebih berhati-hati dalam melakukan komunikasi dengan orang lain dan jangan mudah untuk mempercayai suatu lembaga yang baru dikenal lewat internet. Dan berhati-hatilah dalam melakukan transaksi yang mengharuskan memberikan dan meletakkan nomor kartu kredit dalam berbelanja online tersebut, dikarenakan banyak sekali kejahatan yang berada di dunia maya salah satunya carding. Kesimpulannya, kasus carding di

Indonesia baru bisa diatasi dengan regulasi lama yaitu Pasal 362, 378 dalam KUHP dan Pasal 31 ayat (1) dan (2) dalam UU ITE. Penanggulangan kasus carding memerlukan regulasi yang khusus mengatur tentang kejahatan carding agar kasus-kasus seperti ini bisa berkurang dan bahkan tidak ada lagi. Tetapi selain regulasi khusus juga harus didukung dengan pengamanan sistem baik software maupun hardware, *guidelines* untuk pembuat kebijakan yang berhubungan dengan computer-related crime dan dukungan dari lembaga khusus.

Oleh sebab itulah pembahasan mengenai kejahatan kartu kredit di zaman modern ini Penulis anggap perlu untuk dibahas dalam tulisan ini. Dari uraiandiatas Penulis hendak mengangkat beberapa permasalahan kejahatan kartu kredit ke dalam bentuk skripsi **“TINJAUAN YURIDIS KRIMINOLOGIS TINDAK PIDANA PEMALSUAN KARTU KREDIT DIHUBUNGAN DENGAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK”**

B. Identikasi Masalah

Berkaitan dengan latar belakang diatas, maka penulis mengidentifikasi masalahnya sebagai berikut:

1. Bagaimana hukum pidana indonesia dapat menjangkau tindak pidana pemalsuan kartu kredit ?
2. Faktor apa yang menyebabkan terjadinya pemalsuan kartu kredit ?
3. Upaya apakah yang dapat dilakukan untuk menanggulangi kejahatan kartu kredit ?

C. Tujuan Penelitian

- a. Untuk mengetahui dan mengkaji hukum pidana indonesia dalam menjangkau tindak pidana pemalsuan kartu kredit.
- b. Untuk mengetahui dan mengkaji faktor apa yang menyebabkan terjadinya pemalsuan kartu kredit.
- c. Untuk mengetahui upaya yang dapat dilakukan untuk menanggulangi terjadinya kejahatan kartu kredit.

D. Kegunaan Penelitian

Penulisan ini bertujuan serta diharapkan bermanfaat baik secara teoritis maupun secara praktis.

- a. Secara teoritis, diharapkan dapat memberikan sumbangan pemikiran bagi para pihak dalam pengembangan ilmu pengetahuan dan masyarakat luas mengenai efektifitas Kitab-Kitab Undang Pidana

(KUHP) dan Undang-undang Nomor 11 Tahun 2008 Tentang informasi dan transaksi elektronik dalam penjatuhan sanksi dalam perkara tindak pidana pemalsuan kartu kredit.

- b. Secara Praktis, diharapkan dapat memberikan informasi, masukan mengenai cara mengatasi disparitas penjatuhan sanksi dalam perkara tindak pidana pemalsuan kartu kredit dan manfaat bagi mahasiswa/ i dibidang hukum khususnya, serta pemerintah maupun masyarakat pada umumnya. Dapat memberikan masukan bagi pemerintah, aparat penegak hukum, Asosiasi Kartu Kredit Indonesia (AKKI), dan masyarakat tentang hal-hal yang harus dilakukan dalam upaya menanggulangi kejahatan yang berkaitan dengan kartu kredit dengan menggunakan sarana hukum pidana.

E. Kerangka Pemikiran

Dalam Pembukaan Undang-Undang Dasar Negara republik Indonesia Tahun 1945 alinea keempat, terdapat dasar Negara republik Indonesia yaitu Pancasila. Berkaitan dengan hal itu, H. R. Otje Salman mengatakan bahwa:⁷

“Pembukaan alinea keempat menjelaskan tentang Pancasila yang terdiri dari lima sila. Pancasila secara substansial merupakan konsep yang luhur dan murni; Luhur, karena mencerminkan nilai-nilai bangsa yang diwariskan turun temurun dan abstrak. Murni karena kedalaman substansi yang menyangkut beberapa aspek pokok, baik agamis, ekonomi, ketahanan, sosial, dan budaya yang memiliki corak partikular.”

⁷ Otje Salman dan Anthon F. Susanto, *Teori Hukum (Mengingat, Mengumpulkan, dan Membuka Kembali)*, Refika Aditama, Bandung, 2007, hlm. 158.

Status konstitusi sebagai suatu formal rule yang tertinggi dan sebagai the formal main standard bagi segala aturan serta kehidupan bangsa dan negara. Berkaitan dengan hal tersebut Padmo Wahjono mengatakan bahwa:

“Undang-undang dasar suatu negara selain merupakan dasar dari semua peraturan (*tertulis*) yang ada (*Grundnorm*), maka ia merupakan pula sumber mengalirnya peraturan perundangan terutama apabila kita lihat dari segi materi yang diaturnya. Ringkasnya ia merupakan sumber hukum (*Ursprungsnorm*)”

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang merupakan suatu hukum dasar bagi negara (*Grundnorm*) dijadikan suatu acuan dalam pembentukan hukum selanjutnya, yaitu seperti dalam pembentukan Undang-Undang, Peraturan Pemerintah dan seterusnya.

Pasal 27 ayat (3) Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) kembali hangat diperbincangkan. Kalangan akademisi, politikus, dan aktivis *social networking* kembali memperdebatkan tentang esensi dari pasal yang memidanakan pencemaran nama baik dan penghinaan melalui media internet.

Bagi kubu yang pro Pasal 27 ayat UU ITE, pasal ini berfungsi untuk melindungi hak orang yang dicermakan nama baiknya atau dihina melalui media internet. Bagi kubu yang kontra, pasal ini rumusnya dianggap sebagai jaring empuk untuk membungkan kritik atau bahkan

kebebasan berkespresi di internet. Polemik ini pun berujung pada dilakukannya *judicial review*, dan dalam putusannya Mahkamah Konstitusi (selanjutnya disebut MK) menolak bahwa pasal ini bertentangan dengan Undang-undang Dasar 1945 (selanjutnya disebut UUD 45).

Hukum di Indonesia, khususnya yang tertuang dalam KUHP memuat setidaknya 8 kaliber penghinaan, adapun “kaliber” penghinaan dalam KUHP adalah sebagai berikut:

1. pencemaran nama baik secara lisan [Pasal 310 Ayat (1)];
2. pencemaran nama baik secara tertulis [Pasal 310 Ayat (2)];
3. fitnah (Pasal 311 – 314);
4. penghinaan ringan (Pasal 315);
5. pengaduan fitnah (Pasal 317);
6. menimbulkan persangkaan palsu (Pasal 318);
7. penghinaan terhadap orang mati secara lisan (Pasal 320); dan
8. penghinaan terhadap orang mati secara tertulis (Pasal 321)

Jauh sebelum perdebatan tentang Pasal 27 ayat (3) UU ITE, beberapa ahli hukum juga berbedan pendapat tentang perlu atau tidaknya dibuat Undang-undang yang membuat aturan tentang pidana dengan media internet. Beberapa ahli mengatakan tidak perlu menggunakan Undang-undang baru untuk memidanakan seseorang, karena secara jelas Kitab Undang-undang Hukum Pidana (selanjutnya disebut KUHP) masih relevan, sehingga rumusan KUHP ditafsirkan dengan penafsiran ekstensif

pada kejahatan yang menggunakan media internet, pendapat ini dilontarkan oleh Mardjono Reksodiputro.⁸ Beberapa contohnya adalah sebagai berikut:

- Pelanggaran kesusilaan: 282, 283, 311, 506 KUHP
- Perjudian: 303 KUHP
- Pencemaran nama baik: contohnya Pasal 310-311 KUHP
- Pemerasan atau pengancaman: 335 dan 369 KUHP
- Penipuan: 372, 378, 379, 386, dan 392 KUHP
- Menyebarkan informasi yang menyesatkan: 160 dan 161 KUHP
- Pengancaman kekerasan: 368 KUHP
- Akses area orang lain tanpa ijin: 167 dan 551 KUHP
- Mencuri dengar/menyadap: 112, 113, 114, 322, 323, dan 431 KUHP
- Membuat tidak dapat dipakainya sarana umum: 408 KUHP
- Pemalsuan dokumen: 263, 264, 266, dan 271 KUHP

Ahli hukum yang lain berpendapat bahwa membuat aturan tentang *cyber law* perlu, mengingat kepastian hukum diranah mayantara perlu dilindungi haknya. Tindak pidana yang menyangkut komputer haruslah ditangani secara khusus, karena cara-caranya, lingkungan, waktu, dan letak dalam melakukan kejahatan komputer adalah berbeda dengan tindak pidana lainnya. Pendapat kedua ini diantaranya dilontarkan oleh J. Sudama Sastroandjojo.⁹

⁸ H. Arsyad Sanusi, *Cybercrime*, Milestone, Jakarta, 2011, hlm. 405

⁹ *ibid*, hlm. 406

Kembali pada Pasal 27 ayat (3) UU ITE, perdebatan (diluar konteks *judicial review*) beberapa akademisi dan praktisi sampai hari ini masih berlangsung. Beberapa pendapat yang mendukung adanya Pasal 27 ayat 3 UU ITE adalah sebagai berikut:

1. Edmon Makarim, (Lembaga Kajian Hukum dan Teknologi, Fakultas Hukum Universitas Indonesia)

Pada pokoknya Edmon Makarim menjelaskan bahwasanya Pasal 27 ayat (3) UU ITE haruslah tetap ada agar sistem elektronik tidak menjadi ajang untuk saling mencemarkan nama baik karena dampaknya bersifat masif.¹⁰ Untuk menggunakan pasal ini, penyidik dan jaksa penuntut umum haruslah dapat membuktikan dua unsur obyektif, yaitu dengan sengaja dan tanpa hak.

2. Muhammad Salahuddien Manggalany, (Wakil ketua Indonesia Security Incident Response Team on Internet Infrastructure)

Pada pokoknya M. Salahuddien tidak sepakat dengan argumentasi bahwa pasal pencemaran (*defamation*) sering digunakan untuk membungkam kritik masyarakat terutama di alam reformasi yang sangat terbuka selama ini. Untuk membuktikan dugaan tersebut harus didukung data yang kuat dan lengkap. Ancaman dalam UU ITE lebih berat dari KUHP adalah karena pertimbangan dampak kerusakan yang dihasilkan oleh pencemaran dengan menggunakan teknologi informasi yang bersifat meluas, jangka panjang dan dapat berulang sehingga kerugian yang

¹⁰ Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Rajawali Pers, Jakarta, 2010, hlm. 302

dialami korban jauh lebih besar (efek amplifikasi) dibandingkan apabila pencemaran terjadi melalui saluran konvensional.¹¹

Sementara itu, pada kubu yang mempertanyakan rumusan pasal tersebut, alasan utamanya karena pasal ini memiliki ketidakjelasan rumusan pasal sehingga sangat rentan terjadi multiinterpretasi. Beberapa pendapat tersebut diantaranya:

1. Sutan Remy Sjahdeini, (Guru Besar Fakultas Hukum Universitas Airlangga)

Pada pokoknya mempertanyakan pencantuman frasa “tanpa hak” dalam pasal tersebut. Alasannya adalah apakah ada otoritas resmi yang memiliki otoritas resmi untuk mengizinkan pihak tertentu untuk mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik. Tidak mungkin sifat melawan hukum dari perbuatan-perbuatan tersebut menjadi terhapus karena ada pihak yang dapat memberikan hak kepada pihak lain untuk mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memuat penghinaan dan/atau pencemaran nama baik, dengan kata lain rumusan tersebut dibuat berlebihan.¹²

2. Adami Chazawi, (Ahli Hukum Pidana Fakultas Hukum Universitas Brawijaya)

¹¹ Arsip Milis Telematika diakses 14 Juli 2011.

¹² Sutan Remy Syahdeini, *Kejahatan dan Tindak Pidana Komputer*, Grafiti, Jakarta, 2009, hlm. 232-233.

Pada pokoknya berpendapat andai kata tidak dirumuskan sebagai penghinaan *lex specialis*, penghinaan melalui media elektronik (internet) tetap bisa menggunakan pasal-pasal penghinaan di KUHP yang sesuai dengan kasusnya, dengan cara menafsirkan misalnya berdasarkan tujuan dari dibentuknya kejahatan penghinaan atau yang lebih ekstrim dengan penafsiran ekstensif. Dengan dicantumkan/disebutkan frasa ”pencemaran dan/atau penghinaan”, bisa terjadi salah menafsirkan – seolah-olah bentuk-bentuk penghinaan selain pencemaran – tidak masuk dalam pengertian/cakupan tindak pidana Pasal 27 Ayat (3) UU ITE. Kedelapan bentuk penghinaan (dalam KUHP) jika dilakukan dengan menggunakan sarana elektronik diancam pidana yang sama yakni maksimum 6 tahun penjara dan/atau denda dengan maksimum Rp 1.000.000.000,00 (satu miliar rupiah). Padahal jika kembali pada azas penghinaan yang dibedakan menjadi 8 macam yang diancam dengan pidana yang berbeda-beda, artinya dibebani tanggungjawab sendiri-sendiri secara berbeda-beda berat ringannya. Lebih fatal lagi jika pertanggungjawaban pidana pada penghinaan ringan disamakan dengan fitnah oleh UU ITE dengan ancaman pidana yang sama, yakni maksimum 6 tahun penjara.¹³

Itulah tadi perbedaan pendapat menyikapi rumusan Pasal 27 ayat (3) UU ITE. Secara yuridis, putusan Mahkamah Konstitusi menyatakan bahwa Pasal 27 ayat (3) UU ITE tidak bertentangan dengan UUD 45,

¹³ Adami Chazawi, *Makalah Penghinaan Dalam Hukum Positif di Indonesia*. sam ardi blog, 2009.

tetapi secara akademis, karena dalam konteks keilmuan, sah-sah saja diperdebatkan. Tak kalah pentingnya edukasi terhadap aparat penegak hukum yang *gaptek* a.k.a gagap teknologi bahwa berdasarkan fakta di lapangan pengetahuan mereka tentang kasus yang berhubungan dengan teknologi informasi kurang memadai.

Semakin berkembangnya kejahatan dalam masyarakat, sehingga hukum tjuga harus berkembang agar fungsinya sebagai pemberi rasa aman dapat terpenuhi, dengan adanya undang-undang ini maka diharapkan masyarakat takut untuk melakukan kesalahan, karna dijelaskan pada pada ayat (1), bertanggung jawab atas segala kerugian dan konsekwensi yang timbul, tetapi dalam Undang-Undang ITE pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:

- a) jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi.
- b) jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa; atau
- c) jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.

Pada Pasal 33 menjelaskan bahwa Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya. Juga undang ini barang siapa yang melanggar akan mendapatkan hukuman atau sanksi.

Undang-undang informasi dan elektronik adalah ketentuan yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum indonesia maupun diluar wilayah hukum indonesia, yang memiliki akibat hukum di wilayah hukum indonesia dan diluar wilayah hukum indonesia dan merugikan kepentingan indonesia.

Secara umum, materi undang-undang informasi dan transaksi elektronik (UUITE) dibagi menjadi dua bagian besar, yaitu pengaturan mengenai informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang. Beberapa materi perbuatan yang dilarang (cybercrimes) yang diatur dalam UU ITE, antara lain :

Pasal 27 ayat (1) ”Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.”

(1) Pasal 30 ayat (1) “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.” Ayat (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.” Ayat (3) “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan dengan melanggar, menerobos, melampau, atau menjebol sistem pengamanan.”

Pasal UU ITE yang menjerat kasus penyalahgunaan kartu kredit :

Dalam UU ITE, kasus carding dapat dijerat dengan menggunakan Pasal 31 ayat (1) dan Pasal 31 ayat (2) yang membahas tentang hacking. Karena dalam salah satu langkah untuk mendapatkan nomor kartu kredit pelaku (carder) sering melakukan hacking ke situs-situs resmi lembaga penyedia kartu kredit untuk menembus sistem pengamannya dan mencuri nomor-nomor kartu kredit tersebut.

Pasal 31 ayat (1): "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronika dan atau dokumen elektronik dalam suatu komputer dan atau sistem elektronik secara tertentu milik orang lain."

Pasal 31 ayat (2): "Setiap orang dengan sengaja atau tanpa hak atau melawan hukum melakukan intersepsi atau transmisi elektronik dan atau dokumen elektronik yang tidak bersidat publik dari, ke dan di dalam suatu komputer dan atau sistem elektronik tertentu milik orang lain, baik yang tidak

menyebabkan perubahan, penghilangan dan atau penghentian informasi elektronik dan atau dokumen elektronik yang ditransmisikan.

Dan berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) penyalahgunaan kartu kredit (carding) termasuk dalam Pasal 362 KUHP, dan Pasal 378 KUHP yang merumuskan tentang tindakan pencurian, pemalsuan dan penipuan. Berikut bunyi dan hukuman dalam pasal-pasal tersebut :

Pasal 362 KUHP "Barang siapa mengambil suatu benda yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum". Hukuman : Pidana penjara paling lama 5 tahun atau denda paling banyak sembilan ratus ribu rupiah.

Pasal 378 KUHP "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain dengan melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohongan menggerakkan orang lain untuk menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun menghapuskan piutang." Hukuman : Diancam karena penipuan dengan pidana penjara paling lama 4 tahun.

Apabila diperhatikan Kitab Undang-Undang Hukum Pidana (KUHP),maka tidak ada satu pasal pun yang memberikan rumusan secara jelas dan tegas mengenai batasan kejahatan, Kitab Undang-Undang Hukum Pidana hanya memberikan rumusan perbuatan manakah yang dapat dianggap sebagai suatu kejahatan, misalnya:Pasal 338 KUHP: “ Barang siapa dengan sengaja menghilangkan jiwa orang lain,dihukum, karena makar mati, dengan hukuman

penjara selama-lamanya limabelas tahun". Tetapi walaupun demikian, para sarjana tetap memberikan suatu batasan mengenai kejahatan, antara lain:

W.A Bonger dalam Soerjono Soekanto dkk., *Kriminologi Suatu Pengantar*, mengemukakan bahwa :

kejahatan merupakan perbuatan anti sosial yang secara sadar mendapat reaksi dari negara berupa pemberian derita dan kemudian sebagai reaksi terhadap rumusan-rumusan hukum (legal definitions) mengenai kejahatan.¹⁴

Sedangkan Sue Titus Reid, bagi suatu perumusan hukum tentang kejahatan, maka hal-hal yang perlu diperhatikan antara lain, adalah:

1. kejahatan adalah suatu tindakan sengaja (omisi). Dalam pengertian ini seseorang tidak dapat dihukum hanya karena pikirannya, melainkan harus ada suatu tindakan atau kealpaan dalam bertindak. Kegagalan untuk bertindak dapat juga merupakan suatu kejahatan, jika terdapat suatu kewajiban hukum bertindak dalam kasus tertentu. Disamping itu pula, harus ada niat jahat (criminal intent atau mensrea),
2. merupakan pelanggaran hukum pidana,
3. yang dilakukan tanpa adanya suatu pembelaan atau pembenaran yang diakui secara hukum,¹⁵

Selanjutnya Sutherland, menekankan bahwa :

ciri pokok dari kejahatan adalah perilaku yang dilarang oleh negara, oleh karena merupakan perbuatan yang merugikan negara dan terhadap perbuatan itu negara bereaksi, dengan hukuman sebagai suatu upaya pamungkas.¹⁶

R. Soesilo, mengemukakan bahwa :

secara yuridis pengertian kejahatan adalah suatu perbuatan atau tingkah laku yang bertentangan dengan undang-undang. Untuk dapat melihat apakah perbuatan itu bertentangan dengan undang-undang, maka undang-undang itu haruslah diciptakan terlebih dahulu sebelum adanya peristiwa pidana. Hal ini selain untuk mencegah adanya tindakan yang sewenang-wenang dari pihak penguasa juga agar dapat memberikan kepastian hukum.¹⁷

¹⁴ Soerjono Soekanto, Hengkre Liklikuwata dan Mulyana W. Kusumah, *Kriminologi Suatu Pengantar*, Ghalia Indonesia, Jakarta, 1986, hlm.21

¹⁵ *Ibid*, hlm. 21-22

¹⁶ *Ibid*

¹⁷ M. Ridwan dan Edi Warman, *Azas-azas Kriminologi*, USU Press, Medan, 1994, hlm.45

Ridwan dan Edi Warman mengatakan bahwa kejahatan terutama merupakan pengertian hukum, yaitu:

perbuatan yang dapat dipidana oleh hukum pidana. Tetapi kejahatan bukan semata-mata merupakan batasan undang-undang, artinya: ada perbuatan-perbuatan tertentu yang oleh masyarakat dipandang sebagai “jahat” tetapi Undang-undang tidak menyatakan sebagai kejahatan (tidak dinyatakan sebagai tindak pidana), begitu juga sebaliknya. Dalam hukum pidana orang seringkali membedakan antara “delik-delik hukum” (*rechts delicten* atau *mala per se*) khususnya tindak pidana yang disebut “kejahatan” (Buku II KUHP) dan “delik undang-undang” (*wets delicten* atau *mala prohibita*) yang merupakan “pelanggaran” (Buku III KUHP).¹⁸

Menurut saya sebagai mahasiswa fakultas hukum berpendapat bahwa:

Kejahatan adalah perbuatan yang merugikan, sekaligus asusila, perbuatan mana yang menghasilkan kegelisahan pada masyarakat, sehingga masyarakat itu berhak mencela dan menolak perbuatan itu, dan dengan demikian menjatuhkan dengan sengaja nestapa terhadap perbuatan itu.

Pengertian Kejahatan Kartu Kredit.

- a. Menurut Johannes Ibrahim kejahatan kartu kredit merupakan salah satu bentuk kejahatan bisnis. Memahami makna kejahatan bisnis perlukiranya untuk mencermati perkembangan yang terjadi dalam praktik bisnis dengan berbagai modus, diantaranya adalah dalam bidang kompetisi yang dikenal dengan *unfair competition* (persaingan curang) berupa tindakan *typing contract*, *exclusive dealing*, *price discrimination*, *price fixing*, penggabungan perusahaan, *false advertising* (penipuan iklan) dan kejahatan lingkungan hidup (*environment crime*).
- b. Menurut F.N Jovan kejahatan kartu kredit dikenal dengan istilah *carding*, yaitu penipuan dengan menggunakan data kartu kredit dalam perdagangan di internet.

¹⁸ *Ibid*, hlm. 74

- c. Menurut Ade Ary Sam Indrani kejahatan kartu kredit adalah suatu bentuk kejahatan yang menggunakan kartu kredit orang lain untuk dibelanjakan tanpa sepengetahuan pemiliknya.
- d. Secara umum kejahatan kartu kredit adalah aktifitas pembelian barang di internet menggunakan kartu kredit bajakan.

Teori kriminologis tindak pidana pemalsuan kartu kredit mencakup pada pembahasan Etiologi Kriminal, yang membahas teori-teori yang menyebabkan terjadinya tindak pidana pemalsuan kartu kredit, kriminologis dapat di bagi dalam dua golongan yaitu kriminologis teoritis dan kriminologis praktis terhadap pemalsuan kartu kredit. Kriminologis teoritis Secara teoritis kriminologis dapat dipisahkan kedalam lima cabang pengetahuan. Tiap-tiap begiannya memperdalam pengetahuannya mengenai sebab-sebab kejahatan secara teoritis dari tindak pidana pemalsuan kartu kredit tersebut dengan cara melihat secara antropologi kriminal dan sosiologi kriminal. Kriminologis praktis ilmu pengetahuan yang berguna untuk memberantas kejahatan yang timbul di dalam masyarakat dalam menanggulangi tindak pidana pemalsuan kartu kredit. Kriminologi merupakan ilmu pengetahuan yang mempelajari tentang kejahatan, Pelaksanaan hukuman telah banyak membawa kesuksesan berupa terjaminnya keseimbangan di dalam kehidupan masyarakat. Dalam Pasal 10 Kitab Undang-Undang Hukum Pidana (KUHP) ditentukan dua macam hukuman yaitu hukuman pidana pokok berupa hukuman pidana mati, penjara, kurungan, denda dan hukuman tutupan; dan hukuman pidana tambahan seperti pencabutan hak-hak tertentu, perampasan barang serta

pengumuman keputusan hakim. Kriminologis tindak pidana pemalsuan kartu kredit ini dapat timbul kapan saja di kalangan masyarakat dan kriminologi ini pula yang berusaha untuk memberantas faktor penyebab timbulnya kejahatan pemalsuan kartu kredit dengan cara meningkatkan penyuluhan dan penyediaan sarana oleh negara.

F. Metode Penelitian

Dalam Penelitian ini penulis mempergunakan metode penelitian yang meliputi beberapa hal:

1. Spesifikasi Penelitian

Dalam melakukan penelitian ini penulis menggunakan spesifikasi penelitian deskriptif analitis, yang pada dasarnya menggambarkan permasalahan-permasalahan tindak pidana pemalsuan kartu kredit yang menjadi objek penelitian berdasarkan data yang di peroleh pada saat penelitian ini dilaksanakan. Dalam hal ini menurut pendapat Soerjono Soekanto, penelitian deskriptif dimaksudkan untuk memberikan data yang diteliti, yang artinya mempertegas hipotesa, yang dapat membantu teori-teori lama atau dalam rangka menyusun teori-teori baru. Kegiatan penelitian ini dipergunakan tipologi penelitian hukum normatif, yaitu penelitian yang mempergunakan data sekunder.¹⁹

2. Metode Pendekatan

¹⁹ Soerjono Soekanto, *Pengantar Penelitian Hukum*, Universitas Indonesia, Raja Grafindo Persada, Jakarta, 2010, hlm. 9

Dalam penelitian ini penulis mempergunakan metode pendekatan secara penelitian hukum normatif (yuridis-normatif), yakni merupakan pendekatan atau penelitian hukum dengan menggunakan metode pendekatan/ teori/ konsep dan metode analisis yang termasuk dalam disiplin ilmu hukum yang dogmatis. Dengan menginvertasirisir hukum positif yang berkaitan dengan hukum pidana di bidang kejahatan pemalsuan kartu kredit dan dengan menganalisa putusan pengadilan negeri untuk mengetahui bagaimana penerapan ketentuan hukum pidana terhadap tindak pidana yang berkaitan dengan kartu kredit.

3. Tahap Penelitian

Dalam tahap penelitian ini hanya menekankan pada dua tahapan, yaitu jenis data yang hendak dipergunakan adalah studi kepustakaan:

- a. Penelitian Kepustakaan yaitu dimulai dengan pengumpulan data serta teori-teori dan pendapat para ahli hukum yang berkaitan dengan penentuan sanksi oleh hakim yang menyebabkan terjadinya disparitas dalam perkara tindak pidana pemalsuan data kartu kredit yang berkaitan dengan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Meliputi:
 1. Bahan hukum primer, yaitu: semua dokumen peraturan yang mengikat dan ditetapkan oleh pihak-pihak yang berwenang. Yakni berupa KUHP dan undang-undang.
 2. Bahan hukum sekunder, yaitu: semua dokumen yang merupakan informasi atau hasil kajian tentang kejahatan yang berkaitan dengan

kartukredit, seperti seminar hukum, majalah-majalah, karya tulis ilmiah tentang kejahatan yang berkaitan dengan kartu kredit, dan beberapa sumber dari situs internet yang berkaitan dengan persoalan di atas.

3. Bahan hukum tersier, yaitu: semua dokumen yang berisi konsep-konsep dan keterangan-keterangan yang mendukung bahan hukum primer dan bahan hukum sekunder seperti kamus, ensiklopedia, bibliografi, dan lain-lain.
- b. Penelitian lapangan yaitu dengan melihat fakta-fakta yang terjadi dalam pelaksanaan aturan Perundang-undangan dalam praktiknya.

4. Tahap Pengumpulan Data

Tahap pengumpulan data dalam penelitian ini difokuskan dengan studi dokumen terhadap data sekunder yang kemudian dihubungkan dengan penelitian dilapangan, yaitu dengan meneliti fakta-fakta yang ada dimasyarakat kemudian dikaji sesuai dengan objek penelitian, diantaranya:

a. *Library research* (penelitian kepustakaan), diantaranya dari:

- 1) UUD 1945 Amandemen I-IV.
- 2) Kitab Undang-Undang Hukum Pidana (KUHP).
- 3) Kitab Undang-Undang Hukum Acara Pidana(KUHAP).
- 4) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik..
- 5) Buku-buku atau tulisan karya ilmiah para ahli.
- 6) Majalah, koran dan sumber-sumber lain yang mendukung penelitian ini.

b. *Field research* (penelitian lapangan)

Melakukan interview kepada pihak Pengadilan Negeri Bandung berkaitan dengan disparitas penjatuhan sanksi dalam perkara tindak pidana pemalsuan kartu kredit.

5. Alat Pengumpulan Data

Alat adalah sarana yang dipergunakan untuk pengumpulan data dalam penulisan hukum. Alat pengumpulan data yang dipergunakan dalam penulisan skripsi ini yaitu:

a. Penelitian Kepustakaan

Alat yang digunakan dalam penelitian kepustakaan yaitu pulpen, buku dan alat penghapus.

b. Penelitian Lapangan

Teknik pengumpulan data dengan cara wawancara dengan menggunakan *tipe recorder*.

6. Analisis Data

Penelitian ini mempergunakan metode analisis data yuridis kualitatif, yaitu sebagai cara untuk menarik kesimpulan dari hasil penelitian yang terkumpul. Yuridis, mengingat bahwa penelitian ini bertitik tolak dari peraturan perundang-undangan yang ada sebagai norma hukum normatif. Kualitatif, dimaksudkan bahwa analisis datanya bertitik tolak pada usaha-usaha penemuan asas-asas dan informasi-informasi hukum yang terungkap di dalam penelitian ini, dengan tidak mempergunakan angka-angka, daftar tabel maupun rumusan statistik.

| | | | | | | |
|----|-------------------------------------------------------------|---|---|---|---|---|
| 1 | Persiapan/ Penyusunan Proposal | ■ | ■ | | | |
| 2 | Seminar Proposal | | ■ | ■ | | |
| 3 | Persiapan Penelitian | | | | ■ | |
| 4 | Pengumpulan Data | | | | ■ | |
| 5 | Pengolahan Data | | | | ■ | |
| 6 | Penyusunan Hasil Penelitian Ke Dalam Bentuk Penulisan Hukum | | | | | ■ |
| 7 | Sidang Komprehensif | | | | | ■ |
| 8 | Perbaikan | | | | | ■ |
| 9 | Penjilidan | | | | | ■ |
| 10 | Pengesahan | | | | | ■ |