BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi disuatu Negara dapat dilihat dengan adanya fenomena kemajuan teknologi informasi dan globalisasi yang berlangsung hampir di setiap kehidupan. Teknologi informasi dapat dinilai sebagai simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dari aspek sosial, budaya, ekonomi, dan keuangan. Sebagai negara yang tengah berkembang, Indonesia selalu mengadaptasi berbagai teknologi informasi hingga akhirnya ditemukan internet pada awal abad ke-20 sebagai salah satu wujud perkembangannya. Internet sendiri memiliki fungsi positif yang dapat membantu kehidupan manusia sehari-harinya. Berbagai macam layanan disediakan oleh internet yang bertujuan untuk memudahkan manusia untuk mencapai keinginan serta kebutuhan hidupnya, layanan tersebut diantaranya adalah berupa, *E-Banking*, *E-Goverment*, *E Learning* dan *E-Commerce*.[1]

Salah satu jenis kejahatan yang ditimbulkan oleh kemajuan dan perkembangan teknologi adalah kejahatan yang berkaitan dengan pemanfaatan aplikasi dari internet. Penyalahgunaan internet banyak sekali terjadi dan dapat berubah menjadi sarana untuk melakukan kejahatan atau tindak pidana. Jenis kejahatan yang semula dapat dikatakan sebagai kejahatan konvensional seperti pencurian, pengancaman, pencemaran nama baik bahkan pembobolan mesin

[1]Shali Nurjanah, *KajianYuridisTerhadap Perlindungan Hukum Bagi Nasabah Terhadap Pengambilan Dana Nasabah Melalui Rekening Bank Dengan Sarana Internet*, Skripsi, 2012 Hlm.1-2

Anjungan Tunai Mandiri (ATM) dapat beralih dengan menggunakan internet sebagai sarana untuk melakukan kejahatan dengan resiko minim untuk tertangkap oleh pihak yang berwajib dan situs di internet (*website*) dapat digunakan sebagai media perantara untuk melakukan transaksi melalui internet. Kejahatan yang terjadi apabila tidak terselesaikan pada akhirnya akan mengancam kelangsungan hidup masyarakat, ketertiban hidup dalam bermasyarakat dan keamanan akan terganggu. Dalam kondisi seperti inilah hukum berperan dalam mengatasi benturan-benturan yang terjadi.[2]

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia Internasional. Volodymyr Golubev menyebutnya sebagai *the new form of anti-social behavior* (bentuk baru dari perilaku anti-sosial). *Cybercrime* merupakan satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini.[3]

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

---

[2]Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara,* RefikaAditama, Bandung, 2005, hlm. 47

[3]Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber crime di Indonesia*, Rajawali Pers, Jakarta, 2006, hlm. 1.

macam lainnya. Pelaku *cybercrime* memiliki latar belakang kemampuan yang tinggi dibidangnya sehingga sangat sulit untuk melacak dan memberantasnya secara tuntas.[4]

Hukum pidana Indonesia yang mengatur mengenai *cybercrime* terdapat dalam Undang-undang Nomor 19 tahun 2016 atas perubahan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau yang biasa kita sebut dengan UU ITE. Undang-undang yang telah lahir sejak tiga belas tahun yang lalu ini dirasa masih belum terlaksana secara optimal sampai sekarang. Hal tersebut dikarenakan sejak berlakunya Undang-Undang ITE kejahatan *cyber* tidak berkurang justru cenderung bertambah. Faktor penyebab bertambahnya *cybercrime* bisa dikatakan tidak hanya karena kurang optimalnya pemberlakuan UU ITE tetapi juga karena para penegak hukum belum optimal menangani kasus *cybercrime*, serta kesadaran masyarakat sendiri yang masih rendah mengenai hukum *cyber*.

Bentuk kejahatan *cybercrime* yang marak terjadi adalah kejahatan perbankan, baik berupa pembobolan rekening maupun penyalahgunaan kartu kredit milik orang lain. Untuk penyalahgunaan kartu kredit ini biasanya pelaku kejahatan menggunakan modus *carding*. *Carding* tidak bisa disamakan dengan pencurian kartu kredit pada umumnya. Hal ini dikarenakan para pelaku *carding* atau biasa disebut dengan *carder*, melakukan kejahatan ini tanpa harus mengambil atau menguasai secara fisik kartu kredit milik korban. Pelaku cukup mengetahui nomor kartu kredit milik korban untuk selanjutnya dapat digunakan transaksi

[4]Budi Suhariyanto, *Tindak Pidana Tekologi Informasi (cyber crime)*, Rajawali Pers, Jakarta, 2013, hlm.7.

belanja online sehingga yang dirugikan adalah pemilik kartu kredit yang asli, kejahatan seperti ini disebut kejahatan modus *carding*.[5]

Kerugian yang dialami pengguna internet *banking* memang penyebabnya bervariasi, tapi tetap saja diperlukan legalitas hukum atau aturan perundangan yang baik dan pasti untuk memberikan perlindungan bagi para nasabah pengguna jasa layanan internet *banking*. Dalam rangka menjaga faktor keamanan serta perlindungan hukum bagi nasabah, pemerintah membentuk suatu Undang-Undang yang dapat memberikan perlindungan dan kepastian hukum dalam penyelenggaraan sistem elektronik yakni Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang selanjutnya disebut UU ITE. Pasal 15 ayat (1) Undang-Undang ITE menyatakan bahwa, "setiap penyelenggara elektronik harus menyelenggarakan sistem elektronik secara handal dan aman secara bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya.[6]

Selain payung hukum di atas, terdapat aturan hukum lain yang dapat dijadikan landasan hukum dan sesuai dengan asas, fungsi dan tujuan perbankan Indonesia yang disebutkan dalam, Pasal 2 Undang-Undang No. 7 Tahun 1992 sebagaimana telah diubah dengan Undang-Undang No. 10 Tahun 1998 tentang Perbankan, bahwa "Perbankan Indonesia dalam melakukan usahanya berasaskan demokrasi ekonomi dengan menggunakan prinsip kehati-hatian". Sebagai peraturan pelaksananya kemudian dikeluarkan Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tanggal 30 November 2007 tentang Penerapan Manajemen

[5]Irman S, *Anatomi Kejahatan Perbankan*, MQS Publishing, Bandung, 2006, hlm.161.
[6] Shali Nurjanah, *Op.Cit*, Hlm. 9-11.

Resiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum. Manajemen resiko pada aktifitas pelayanan jasa bank melalui internet (Internet *Banking*) mengatur tentang penyelenggaraan sistem elektronik perbankan, dimana pelaksanaannya diserahkan kepada masing-masing bank. Dalam surat edaran tersebut Bank Indonesia hanya memberikan pedoman sehingga dalam pelaksanaannya tidak merugikan nasabah dan bank itu sendiri. Selain adanya peraturan mengenai perlindungan hukum diatas, berdasarkan peraturan perundang-undangan yaitu UU ITE, pelaku pencurian dana nasabah bank dapat dikenai sanksi pidana berdasarkan pasal 32 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun baik memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak." Pasal-pasal dalam UU ITE tersebut dapat diindikasikan sebagai pasal yang mengatur mengenai perbuatan pencurian rekening bank melalui sarana internet, akan tetapi jika dikaji lebih dalam lagi, unsur-unsur yang terdapat pada pasal UU ITE pasal 32 ayat (2) ini masih dirasa kurang untuk memenuhi unsur-unsur yang terdapat di dalam perbuatan yang merugikan para nasabah bank.

Untuk menunjang pasal-pasal dalam UU ITE tersebut, maka pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP), dapat digunakan untuk menjerat pelaku kejahatan pencurian rekening bank melalui sarana internet, yang begitu rinci mengurai unsur-unsur perbuatan mengenai pencurian. Hal ini tentu saja menarik perhatian penulis untuk mengkaji lebih dalam mengenai perlindungan

hukum UU ITE terhadap korban pencurian rekening bank melalui internet.[7]

Pada Pasal 362 hukumannya paling lama hanya 5 tahun penjara, sedangkan jika dikenakan Pasal 30 UU ITE, pidananya lebih berat sebagaimana diatur dalan Pasal 30 UU ITE yang berbunyi:

(1) Setiap Orang dengan sengaja dan tanpa hak atau 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.

Ancaman hukuman dari Pasal 30 UU ITE yang dijelaskan dalam Pasal 46 yang bunyinya :

(1) "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)".
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah".

Sejak munculnya Undang-Undang Informasi Tentang Elektronik banyak menimbulkan pro dan kontra dalam masyarakat karena memang ada beberapa pasal dalam Undang-Undang ITE dianggap membatasi kebebasan masyarakat yang ingin menyampaikan aspirasinya ataupun pendapatnya lewat dunia maya. Salah satu pasal yang bermasalah masih terkait dengan pasal 27 ayat 3 tentang

[7]*Ibid*., *hlm*.9-11.

kasus pencemaran nama baik atau defamasi, karena pasal ini dapat digunakan untuk membatasi ataupun mengekang masyarakat untuk mengkritik pihak kepolisian dan pemerintah. Pasal tersebut membahas tentang penghinaan dan pencemaran nama baik melalui dunia maya.

Adapun contoh kasus *carding* yang diperiksa dan diadili oleh Pengadilan Negeri Surabaya dengan nomor register perkara 2322/Pid.Sus/2019/PN.Sby. atas nama terdakwa Anggi Affiansyah.

Terdakwa tersebut divonis pidana penjara selama 1 (Satu) tahun dan denda sebesar Rp. 3.000.000,00 (tiga juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama 1 (Satu) bulan. Terdakwa di dakwa dengan Pasal 30 ayat (1) Jo. Pasal 46 ayat (1) UU RI Nomor 19 Tahun 2016 tentang Perubahan Atas UU RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik,"dengan sengaja 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.

Pada kasus dalam 2322/Pid.Sus/2019/PN.Sby., menyatakan bahwa terdakwa Anggi Affiansyah telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana melanggar Pasal 30 ayat (1) Jo. Pasal 46 ayat (1) UU RI Nomor 19 Tahun 2016 atas perubahan UU RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Menjatuhkan pidana terhadap terdakwa tersebut dengan pidana penjara selama 1 (satu) tahun dan denda sebesar Rp3.000.000,00 (tiga juta rupiah) dengan ketentuan apabila denda tersebut tidak

dibayar maka diganti dengan pidana kurungan selama 1 (Satu) bulan. Hakim menetapkan masa penahanan yang telah dijalani oleh terdakwa tersebut. Hakim memutuskan agar terdakwa tetap berada didalam tahanan dan menerapkan barang bukti berupa 1 (satu) unit handphone merk Samsung Note 9 warna hitam, 1 (satu) unit laptop merk Dell Inspiron warna hitam. Membebankan kepada terdakwa membayar biaya perkara sejumlah Rp.5000,00 (lima ribu rupiah).

Hal yang menarik dari kasus tersebut untuk diangkat yaitu kenyataan bahwa sebenarnya tidak adanya pengaturan mengenai *carding* ini sendiri secara langsung yang menyebabkan adanya suatu kekosongan hukum sehingga dapat mengakibatkan banyak sekali kasus semacam ini yang ternyata ditangani secara berbeda-beda, dalam arti penggunaan pasal-pasal yang berbeda untuk menjerat pelaku *carding*, tergantung dari penafsiran penyelidik dan penyidik di tingkat pemeriksaan awal.

Berdasarkan latar belakang yang telah di paparkan di atas, maka penulis ingin melakukan penelitian lebih lanjut dengan judul "**Kebijakan Pidana Dalam Penanggulangan Kejahatan *Carding* Di Tinjau Dari Undang-Undang Nomor 19 Tahun 2016 Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik.**"

B. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka dapat dikemukakan rumusan masalah sebagai berikut:

1. Apakah faktor penyebab terjadinya kejahatan *carding* ?

2. Bagaimanakah kebijakan hukum terhadap kejahatan *carding* sebagai bentuk *cyber crime* ditinjau dari Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik ?

C. Tujuan Penelitian

1. Penelitian ini dilakukan untuk mengetahui faktor yang menjadi penyebab terjadinya kejahatan *carding.*
2. Penelitian ini dilakukan untuk mengetahui bagaimana kebijakan hukum berperan terhadap tindak pidana kejahatan *carding*.

D. Manfaat penelitian

1. Secara Teoritis, hasil penelitian ini diharapkan dapat memberikan sumbangan pemikiran untuk ilmu pengetahuan hukum pidana di Indonesia khususnya mengenai Tindak Pidana penipuan kartu kredit atau disebut juga *Carding* dan pengkajian ini diharapkan dapat memberikan gambaran umum secara yuridis bahwa fenomena kejahatan penipuan kartu kredit yang semakin canggih dan mengacu pada dampak yang terjadi dikemudian hari.
2. Secara Praktis, untuk hasil dari penelitian ini diharapkan dapat memberikan solusi atau jalan keluar bagi objek masalah yang sedang diteliti untuk dapat diimplementasikan dalam kehidupan sehari-hari, kemudian diharapkan mampu memberikan penjelasan bagi masyarakat serta pihak lain untuk dapat memahami dan mengetahui persepktif yuridis mengenai objek masalah yang diteliti.

E. Tinjauan Pustaka

1. Pengertian Kebijakan Hukum Pidana

Istilah kebijakan berasal dari bahasa Inggris *policy* atau dalam bahasa Belanda *politie*. Secara umum kebijakan dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah dalam mengelola, mengatur atau menyelesaikan urusan-urusan publik, masalah-masalah masyarakat atau bidang-bidang penyusunan peraturan perundang-undangan dan pengaplikasian hukum/peraturan, dengan suatu tujuan yang mengarah.

Upaya perlindungan masyarakat (*social defence*) dan upaya mencapai kesejahteraan masyarakat (*social welfare*) pada hakikatnya merupakan bagian integral dari kebijakan atau upaya penanggulangan kejahatan.[8]

Pengertian kebijakan atau politik hukum pidana dapat dilihat dari politik hukum maupun politik kriminal. Menurut Sudarto, "Politik Hukum" adalah :

1. Usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat nanti
2. Kebijakan dari negara melalui badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan.[9]

Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya juga merupakan bagian dari usaha penegakkan hukum (khususnya penegakkan hukum pidana). Oleh karena itu, sering pula dikatakan bahwa politik atau

[8] Barda Nawawi Arief, Bunga Rampai . 2013 . *Kebijakan Hukum Pidana*, Bandung : Citra Aditya Bakti . hlm. 32.

[9] Sudarto. 2012 . *Hukum dan Hukum Pidana*, Jakarta : Rajawali pers . hlm. 44-48.

kebijakan hukum pidana merupakan bagian pula dari kebijakan penegakkan hukum (*law enforcement policy*).[10]

2. Pengertian dan Ruang Lingkup Cyber Crime

Sebelum membahas apa itu pengertian kejahatan *cyber* (*cybercrime*) secara terperinci, maka terlebih dahulu akan dijelaskan induk kejahatan siber (*cybercrime*) yaitu *cyberspace*. *Cyberspace* dipandang sebagai sebuah dunia komunikasi berbasis komputer. Dalam hal ini, *cyberspace* dianggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan internet.

Realitas baru ini dalam kenyataannya terbentuk melalui jaringan komputer yang menghubungkan antar negara atau antar benua yang berbasis protokol. Hal ini berarti dalam sistem kerjanya dapatlah dikatakan bahwa internet (*cyberspace*) telah mengubah jarak dan waktu tidak terbatas. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda.[11]

Dalam perkembangan selanjutnya, kehadiran teknologi canggih komputer dengan jaringan 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. Internet telah mampu membuka cakrawala baru dalam kehidupan manusia baik dalam konteks sarana komunikasi dan informasi yang

[10] Barda Nawawi Arief, Bunga Rampai……,*Op. cit*., hlm. 28
[11] Maskun, *Kejahatan Siber (Cybercrime)*, Kencana, Jakarta, 2013, hlm. 46.

menjanjikan menembus batas-batas negara maupun penyebaran dan pertukaran ilmu pengetahuan dan gagasan di kalangan ilmuan di seluruh dunia.[12]

Cybercrime di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer, akan tetapi melibatkan teknologi telekomunikasi didalam pengoperasiannya. Hal ini dapat dilihat dari pandangan Indra Safitri yang mengemukakan kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta 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.[13]

3. Jenis-Jenis *Cyber Crime*

Berdasarkan motif kegiatannnya, *cybercrime* dapat digolongkan sebagai berikut:

1. *Cybercrime* sebagai tindakan kejahatan murni yaitu, kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah *Carding*, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (*webserver, mailing list*) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (*spamming*) juga dapat dimasukkan dalam contoh kejahatan yang

[12]Widyopramono Hadi Widjojo, *Jurnal Hukum Teknologi:Cyber Crime dan Pencegahannya*, Volume 2, Universitas Indonesia, Depok, 2005, hlm. 7.
[13]Maskun, *Op Cit*, hlm. 47-48

menggunakan internet sebagai sarana. Di beberapa Negara maju, pelaku *spamming* dapat dituntut dengan tuduhan pelanggaran privasi.

2. *Cybercrime* sebagai tindakan kejahatan abu-abu pada jenis kejahatan di internet yang masuk dalam wilayah ”abu-abu”, cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah *probing* atau *port scanning*. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, *port-port* yang ada, baik yang terbuka maupun tertutup, dan sebagainya.
3. *Cybercrime* yang menyerang individu (*Againts Person*) yaitu, kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermaikan seseorang untuk mendapatkan kepuasan pribadi. Contoh : Pornografi, *cyberstalking*, dll
4. *Cybercrime* yang menyerang hak cipta/hak milik (*Againts Property*) yaitu, kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi/nonmateri.
5. *Cybercrime* yang menyerang pemerintah (*Againts Government*) yaitu, kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun merusak keamanan suatu pemerintahan

yang bertujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu Negara (*Cyber Terorism*).[14]

4. Pengertian dan Ruang Lingkup *Carding*

Kejahatan *carding* yaitu merupakan kejahatan mencuri data atau informasi kartu kredit orang lain secara ilegal yang digunakan untuk berbelanja online melalui situs-situs belanja di internet maupun berbelanja secara konvensional yang tagihannya dialamatkan kepada pemilik kartu yang sebenarnya dari kartu kredit tersebut. Kejahatan *carding* marak terjadi sebagai akibat dari perkembangan dan kemajuan teknologi informasi dan komunikasi yang mampu membuat masyarakat menjadi khawatir karena kerugian yang ditimbulkannya tidak bisa dianggap sedikit.

Penyebab terjadinya kejahatan *carding* tidak hanya disebabkan karena perkembangan dari teknologi informasi dan komunikasi yang semakin maju namun ada beberapa faktor lain yang ikut berperan menjadi penyebab dari kejahatan *carding*. Penyebab munculnya kejahatan *carding* dibagi menjadi dua faktor yaitu faktor internal dan faktor eksternal yaitu semuanya akan dijelaskan sebagai berikut**.**[15]

Kejahatan *carding* juga merupakan salah satu bagian dari kejahatan *cyber* atau *cybercrime* yaitu kejahatan yang memanfaatkan teknologi canggih sebagai alat untuk mencapai tujuan untuk melakukan kejahatan. *Carding* adalah *cybercrime* dengan cara mencuri data kartu kredit dari nasabah suatu bank, sehingga si pelaku *carding* (*carder*) dapat menggunakan data tersebut untuk

[14] Eliasta Ketaren, *CyberCrime, CyberSpace, Dan CyberLaw,* Jurnal TIMES, Vol. V No.2 : 35-42, 2016

[15] *Ibid*., hlm. 44.

keuntungan pribadi. Tujuan utamanya adalah untuk membelanjakann secara tidak sah kartu kredit yang telah didapatkan ataupun untuk memperoleh dana milik pengguna sah kartu kredit tersebut. Akibat dari kejahatan dunia maya dapat lebih luas daripada tindak pidana konvensional, karena para pelaku tidak dibatasi oleh waktu dan georgafis, oleh karena itu wilayah terjadinya tidak hanya secara lokal atau nasional tetapi juga transnasional dan internasional. Perkembangan kasus *carding* di Indonesia bergerak sangat cepat. Menurut hasil riset terkini yang dilakukan perusahaan sekuriti *Clearcommecre* yang berbasis di Texas, menyatakan bahwa Indonesia berada di urutan pertama negara asal pelaku *Cyber fraud*.[16]

5. Tinjauan Dari Undang-Undang Nomor 19 tahun 2016 Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik.

Tanggal 23 April 2008 telah diundangkan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang- Undang ITE telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang ITE (cybercrime) dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu. Tindak Pidana Cybercrime dalam Undang-Undang ITE diatur dalam 9 pasal, dari pasal 27 sampai dengan pasal 35. Dalam 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang

[16] Endah Lestari, *Tinjauan Yuridis Kejahatan Penggunaan Kartu Kredit di Indonesia, Jurnal Hukum Vol. XVIII No.18*, April 2010 1-16, hal.2

dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 samapai dengan Pasal 34. Sementara ancaman pidananya denda dan pidana penjara ditentukan didalam Pasal 45 sampai Pasal 52. Adapun rumusan pasal- pasal tersebut adalah sebagai berikut :

"Pasal 27 yang berbunyi :

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.
2) 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 perjudian.
3) 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 penghinaan dan/atau pencemaran nama baik.
4) 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 pemerasan dan/atau pengancaman.

"Pasal 28 yang berbunyi :

1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA)."

"Pasal 29 yang berbunyi :

"Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi."

“Pasal 30 yang berbunyi :

1) Setiap Orang dengan sengaja dan tanpa hak atau 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.”

“Pasal 31 yang berbunyi :

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi 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 apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.”

“Pasal 32 yang berbunyi :

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya."

"Pasal 33 yang berbunyi :

"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."

"Pasal 34 yang berbunyi :

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
    a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33
    b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33
2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum."

"Pasal 35 yang berbunyi :

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik."

"Pasal 36 yang berbunyi :

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain."

"Pasal 37 yang berbunyi :

> "Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia."

Dengan kemajuan teknologi yang semakin pesat maka dapat memunculkan kejahatan-kejahatan baru yang timbul akibat dari kemajuan teknologi informasi maka berikut adalah perbandingan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yaitu dimana perubahan terhadap hukum pidana Indonesia berkaitan dengan munculnya kemajuan teknologi informasi sebagai berikut :

TABEL I

PERBANDINGAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 DENGAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

No.	**Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik**.	**Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang- undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.**
1.	Dalam Pasal 1 mengenai ketentuan umum terdapat 23 poin ketentuan-ketentuan umum.	Dirubah dengan penambahan dalam Pasal 1 yakni Pasal 1 diantara angka 6 dan angka 7 disipkan 1 angka yakni angka 6a, ketentuan mengenai Penyelenggara Sistem Elektronik.
2.	Tidak ada Penambahan dan perubahan dibeberapa Dalam Pasal 26, Pasal 31, Pasal 40, Pasal 43,	Dirubah dan ditambahan, dalam Pasal 26 ditambah 3 (tiga) ayat, yakni ayat (3), ayat (4), dan ayat (5); Pasal 31 Ketentuan ayat (3) dan ayat (4) diubah;

		Pasal 40 disisipkan 2 (dua) ayat, yakni ayat (2a) dan ayat (2b) dan ketentuan ayat (6) diubah; Pasal 43 Ketentuan ayat (2), ayat (3), ayat (5), ayat (6), ayat (7), dan ayat (8) diubah dan ditambahkan satu (1) ayat, yakni ayat (7a) serta penjelasan ayat (1) Pasal 43 diubah.
3.	Tidak adanya penjelasan mengenai Pasal 5 tentang alat bukti elektronik	Dirubah dengan penambahan penjelasan dalam Pasal 5
4.	Tidak adanya kewajiban penyelenggara sistem elektronik untuk menghapus Informasi Elektronik yang tidak relevan berdasarkan penetapan pengadilan	Adanya kewajiban penyelenggara sistem elektronik untuk menghapus Informasi Elektronik yang tidak relevan berdasarkan penetapan pengadilan
5.	Segala bentuk penyadapan tidak diperbolehkan	Penyadapan boleh dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan
6.	Dalam hukum acara yang digunakan ada ketentuan khusus dalam hal penggeledahan, penyitaan barang bukti yakni mutlak harus melalui izin pengadilan	Adanya perubahan dalam penggeledahan dan penyitaan barang bukti elektronik dilakukan sesuai dengan ketentuan hukum acara pidana dalam KUHAP
7.	Dalam Pasal 45 mengenai ketentuan pidana tidak ada penambahan pasal. Ancaman pidana penjara untuk Pasal 29 paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).	Dalam pasal 45 dan Pasal 46 disisipkan 2 (dua) pasal, yakni Pasal 45A dan Pasal 45B. Serta perubahan ancaman pidana penjara untuk Pasal 29 dipidanakan menjadi paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah) Terdapat pada Pasal 45B.

F. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian normatif/yuridis normatif (*normative legal research*). Penelitian hukum ini juga sering disebut dengan penelitian hukum doktriner karena penelitian hukum ini ditujukan atau dilakukan hanya pada peraturan-peraturan yang tertulis atau bahkan

hukum yang lain. Dengan demikian, penelitian normatif mempunyai sifat tertutup artinya hanya terbatas pada hukum positif (peraturan perundang-undangan, yurisprudensi, hukum adat, konvensi ketatanegaraan, Dan lain-lain). Metode yang dipergunakan sesuai dengan ilmu mengenai cara-cara mengetahui hukum positif, yaitu metode penafsiran, analogi, konstruksi, perbandingan dan sejarah.[17]

Peter Mahmud Marzuki menjelaskan penelitian hukum normatif adalah suatu proses untuk menemukan suatu aturan hukum, maupun doktrin-doktrin hukum untuk menjawab permasalahan hukum yang dihadapi. Penelitian hukum normatif dilakukan untuk menghasilkan argumentasi, teori atau konsep baru sebagai perskripsi dalam menyelesaikan masalah yang dihadapi.[18]

Penelitian hukum normatif selalu mengambil isu dari hukum sebagai sistem norma yang digunakan untuk memberikan justifikasi deskriptif tentang suatu peristiwa hukum. Sehingga penelitian hukum normatif menjadikan sistem norma sebagai pusat kajiannya. Sistem norma dalam arti yang sederhana adalah sistem kaidah atau aturan. Sehingga penelitian hukum normatif adalah penelitian yang mempunyai objek kajian tentang kaidah atau aturan hukum. Penelitian hukum normatif meneliti kaidah atau aturan hukum sebagai suatu bangunan sistem yang terkait dengan suatu peristiwa hukum. Penelitian normatif hanya berhenti pada lingkup konsepsi hukum, asas hukum dan kaedah hukum peraturan saja, tidak sampai perilaku manusia yang menerapkan peraturan tersebut.[19]

2. Pendekatan Penelitian

---

[17] Fakultas Hukum Universitas Malikussaleh, *Buku Panduan Penulisan Tugas Akhir Skripsi*, Fakultas Hukum, Lhokseumawe, 2019-2020, hlm. 10

[18] *Ibid.*

[19] *Ibid, hlm.13.*

Dalam penelitian ini penulis menggunakan pendekatan konseptual (*conceptual approach*) dan pendekatan perundang-undangan (*statute approach*). Penelitian dengan pendekatan konseptual (*conceptual approach*) adalah penelitian yang dilakukan dengan melihat konsep-konsep tentang penipuan kartu kredit online (*carding*) yang terdapat dalam berbagai literatur. Penelitian dengan pendekatan perundang-undangan (*statute approach*) adalah penelitian dengan yang dilakukan dengan cara menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang ditangani.[20]

3. **Sifat dan Bentuk Penelitian**

Penelitian yang dikaji penulis dalam penelitian ini merupakan penelitian yang bersifat deskriptif, sifat ini dimaksudkan untuk memberikan argumentasi atas hasil penelitian yang telah dilakukannya. Argumentasi disini dilakukan oleh peneliti untuk memberikan deskripsi atau penilaian mengenai benar atau salah atau apa yang seyogyanya menurut hukum terhadap fakta atau peristiwa hukum dari hasil penelitian.

Dari bentuknya penelitian ini termasuk kedalam penelitian deskriptif yaitu penelitian yang dilakukan guna memberikan gambaran atau merumuskan masalah sesuai keadaan atau fakta yang ada.[21]

4. **Sumber Data**

Sumber data dapat dibedakan menjadi 3, yaitu data primer, data sekunder, dan data tersier. Dalam penelitian ini, penulis menggunakan sumber bahan hukum yaitu :

---

[20] Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana Prenada Media Grup, Jakarta, 2011,hlm. 24.

[21] *Ibid, hlm*. 17.

a. Bahan Hukum Primer

Bahan hukum primer yang digunakan terdiri dari peraturan perundang-undangan, catatan resmi, risalah dalam pembuatan perundang-undangan dan putusan hakim.[22] Dalam penelitian ini bahan hukum primer yang digunakan adalah sebagai berikut :

1) Undang-Undang Dasar 1945
2) Kitab Undang-Undang Hukum Pidana
3) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

b. Bahan Hukum Sekunder

Bahan Hukum Sekunder, adalah bahan hukum yang menunjang dan memberikan penjelasan mengenai bahan hukum primer. Dalam penelitian ini bahan hukum primer yang digunakan adalah sebagai berikut :

1) Buku-buku ilmiah dibidang hukum
2) Makalah-makalah
3) Jurnal ilmiah
4) Artikel ilmiah

c. Bahan Hukum Tersier

Bahan Hukum Tersier, adalah bahan-bahan hukum yang menberikan informasi dan penjelasan mengenai bahan hukum primer dan bahan hukum sekunder. Dalam penelitian ini bahan hukum tersier yang digunakan meliputi :

1) Kamus Besar Bahasa Indonesia

[22] Peter Mahmud Marzuki, *Op. Cit*, hlm. 92.

2) Kamus hukum
3) Situs internet/website yg berkaitan dengan penipuan kartu kredit online (*carding*)

5. Teknik Pengumpulan Data

Teknik pengumpulan bahan hukum dimaksudkan untuk memperoleh bahan hukum dalam penelitian. Teknik pengumpulan bahan hukum yang dilakukan dalam penelitian ini adalah melalui teknik penelitian dokumen/literature (*Library Research*). *Library Research* dilakukan peneliti dengan melakukan kajian-kajian atas dokumen pendukung penelitian.

6. Teknik Analisis Data

Analisis data merupakan kegiatan dalam penelitian yang melakukan kajian telaah terhadap hasil pengolahan data yang dibantu dengan teori-teori yang telah didapat sebelumnya. Secara sederhana ini disebut sebagai kegiatan memberikan telaah, yang dapat berarti menentang, mengkritik, mendukung, menambah atau memberi komentar dan kemudian membuat suatu kesimpulan terhadap hasil penelitian dengan pikiran sendiri dan bantuan teori yang telah dikuasai.