BAB I

PENDAHULUAN

A. Latar Belakang

Kemajuan ilmu pengetahuan dan teknologi informasi pada era globalisasi terus berkembang pesat. Indonesia adalah salah satu negara yang tidak luput dari perkembangan teknologi. Adanya perkembangan teknologi informasi membuat interaksi dunia menjadi tanpa batas dan menyebabkan perubahan sosial berlangsung lebih cepat. Perkembangan teknologi komunikasi dan informasi yang sangat cepat ini tentunya memberikan manfaat yang besar bagi kehidupan manusia. Melalui kemajuan teknologi informasi masyarakat memiliki ruang gerak yang lebih luas.

Berbagai bidang kehidupan manusia kini mulai menerapkan berbagai kemajuan teknologi dan informasi,salah satunya dengan penggunaan kartu kredit. Dengan kartu kredit di tangan, semua jadi mudah, gampang dan cepat ketika berbelanja atau membeli tiket pesawat, membayar rekening dan tagihan, dan sebagainya, kini tidak perlu membawa uang dalam jumlah banyak.

Kartu kredit memang memang menawarkan berbagai kemudahan transaksi bagi nasabah penggunanya sehingga nasabah dapat berbelanja dengan banyak tanpa uang *cash*. Penggunaan uang tunai dalam jumlah besar cukup beresiko, seperti resiko kehilangan, pemalsuan serta perampokan. Akibatnya penggunaan uang tunai sebagai alat pembayaran semakin berkurang dan digantikan oleh penggunaan kartu kredit.

Menurut Undang-Undang Nomor 7 Tahun 1972 Sebagaimana Telah Diubah dengan Undang-Undang No. 10 Tahun 1998 tentang Perbankan, Kartu kredit adalah salah satu alat pembayaran paling mutakhir setelah cek dan giro yang bersifat tidak tunai.

Pada prinsipnya kartu kredit diciptakan untuk kemudahan dan cara kerjanya diatur oleh Bank Indonesia (BI) sebagaimana halnya produk perbankan yang lain.

Kemajuan teknologi saat ini terkadang tak hanya dimanfaatkan masyarakat dalam kegiatan positif. Namun, bisa juga dimanfaatkan dengan menjadikan kegiatan negatif seperti dalam perkembangan, kemajuan teknologi juga dijadikan peluang bagi para 'penjahat' untuk melakukan kriminalitas di dunia maya atau media lainnya yang kerap dikenal dengan istilah kejahatan *cybercrime.*

Pengertian *cybercrime* yaitu sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara *ilegal*.[1] *Cybercrime* berasal dari kata *cyber* yang berarti dunia maya atau internet dan *crime* yang berarti kejahatan. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet.

Cybercrime memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas perkembangan *cybercrime* ini.

Dari beberapa macam *cybercrime* yang terjadi di Indonesia yaitu salah satunya *cybercrime* kejahatan *carding* (pembobolan kartu kredit)*, carding* adalah penipuan pada kartu kredit yang mana pelaku mengetahui nomor kartu kredit seseorang yang masih berlaku untuk digunakan, maka pelaku dapat membeli barang secara *online*

[1] Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, 2013, hlm 25

yang tagihannya bisa dialamatkan pada pemilik asli kartu kredit tersebut, sedangkan pelakunya dinamakan *carder.*

Pembobolan kartu kredit *(Carding)* merupakan suatu bentuk kejahatan berbasis teknologi informasi *(Cybercrime*) berupa pembobolan kartu kredit orang lain yang digunakan untuk pembayaran atas transaksi jual beli tanpa izin dan juga tanpa sepengetahuan pemegang *credit card* yang sah. Orang yang melakukan *carding* sering disebut *carder*.[2]

Pada dasarnya kegiatan *carding* dilakukan dengan cara melakukan transaksi bisnis yang kebanyakan adalah aktifitas jual beli secara *online* melalui internet kemudian memasukkan jenis pembayaran dengan tipe kartu kredit dan selanjutnya ketika dikonfirmasi isian informasi kartu kredit pelaku memasukkan informasi kartu kredit orang lain, sehingga tagihan akan masuk ke rekening orang lain.

Pembobolan kartu kredit atau *carding* tentunya sangat merugikan pemilik kartu kredit. Bagi pemilik kartu kredit, akan memperoleh dampak negatif secara nyata. Pemilik kartu kredit akan mendapatkan pencurian atau penggunaan kartu kredit secara ilegal yang digunakan untuk melakukan segala jenis transaksi yang dilakukan oleh *carder.*

Dengan adanya hal tersebut, pemilik kartu kredit tentu akan mengalami kerugian yang sangat dominan. Perbuatan para *carder* yang "mengintip" dan "memanipulasi" atau membobol kartu kredit milik orang lain ini telah melanggar ketentuan yang tedapat dalam peraturan perundang-undangan yang paling khusus, yakni Undang-

[2] H. Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya,* LaksBang PRESS indo, Yogyakarta, 2007, hlm, 10.

Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Berdasarkan hal tersebut penulis tertarik mengangkat penelitian yang berjudul **ANALISIS YURIDIS *CYBERCRIME* DALAM PEMBOBOLAN KAR TU KREDIT (*CARDING*) (Studi Putusan Nomor 1229/Pid.Sus/ 2020/PN.Mks).**

B. Rumusan Masalah

Berdasarkan latar belakang masalah maka dapat dirumuskan permasalahan dalam penelitian ini sebagai berikut :

1. Bagaimana pertanggungjawaban pidana terhadap pelaku *cybercrime* dalam pembobolan kartu kredit (*carding)* dalam putusan nomor 1229/Pid.Sus/20 20/PN Mks?
2. Bagaimana pertimbangan hukum hakim terhadap *cybercrime* dalam pembobolan kartu kredit (*carding)* dalam putusan nomor 1229/Pid.Sus/2020/PN Mks?

C. Tujuan Penelitian

1. Untuk mengetahui pertanggungjawaban pidana terhadap pelaku *cybercrime* dalam pembobolan kartu kredit (*carding)* dalam putusan nomor 1229 /Pid.Sus/2020/PN Mks.
2. Untuk mengetahui dan menganalisis pertimbangan hakim terhadap *cybercrime* dalam pembobolan kartu kredit (*carding)* dalam putusan nomor 1229/Pid.Sus/2020/PN Mks.

D. Manfaat Penelitian

Berdasarkan tujuan penelitian yang hendak dicapai, maka penelitian ini diharapkan mempunyai manfaat dalam pendidikan baik secara langsung maupun tidak langsung. Adapun manfaat penelitian ini adalah sebagai berikut :

1. Secara Teoritis
    a. Hasil penelitian ini diharapkan dapat memberikan sumbangan pemikiran untuk ilmu pengetahuan hukum pidana di Indonesia tentang kejahatan *cybercrime* dalam pembobolan kartu kredit (*carding*).
    b. Diharapkan hasil penelitian ini akan menambah kepustakaan ilmu pengetahuan dan menjadi bahan penelitian hukum pada umumnya dan dalam hukum pidana khususnya.
2. Secara Praktis

Hasil penelitian ini diharapkan dapat digunakan sebagai ilmu tambahan dan masukan bagi aparat penegak hukum khususnya tentang tentang *cybercrime* dalam pembobolan kartu kredit (*carding*).

3. Manfaat Bagi Penulis

Adapun manfaat penelitian ini bagi penulis adalah sebagai salah satu syarat untuk memperoleh gelar Sarjana di Fakultas Hukum Universitas HKBP Nommensen Medan dan menambah pengetahuan mengenai *cybercrime* khususnya dalam pembobolan kartu kredit (*carding).*

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tindak Pidana *Cybercrime*

1. Pengertian *Cybercrime*

Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan.[3] Kemajuan teknologi yang merupakan hasil budaya menusia di samping membawa dampak positif, dalam arti dapat diperdayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan manusia dan peradabannya.

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 (pribadi). Internet telah mampu membuka cakrawala baru dalam kehidupan manusia baik dalam konteks sarana komunikasi dan informasi yang menjanjikan menembus batas-batas negara maupun penyebaran dan pertukaran ilmu pengetahuan dan gagasan di kalangan ilmuan di seluruh dunia.

---

[3]Abdul Wahid dan Mohammad Labib, *Kejahatan Mayaantara (Cybercrime),* Bandung, Refika Aditama 2005, hlm. 23.

Perkembangan internet selain berdampak positif ternyata juga membawa sisi negatif, dengan membuka peluang munculnya tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak terpikirkan akan terjadi. Sebuah teori menyatakan *crime is product of sociaty it self*, yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang menghasilkan kejahatan.

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang khas sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya (penyelidikan, penyidikan hingga dengan penuntutan).[4]

Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime.* Istilah *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan komputer atau jaringan komputer menjadi alat, sasaran, atau tempat terjadinya kejahatan.[5] *Cybercrime* merupakan dimensi baru dari kejahatan masa kini yang menyita perhatian publik internasional.[6]

---

[4] Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kajian Kompilasi),* Jakarta Raja Grafindo Persada 2005, hlm. 426.
[5] Akbar Kurnia Putra, *Harmonisasi Konvensi Cyber Crime Dalam Hukum N*asional, Jurnal Ilmu Hukum Jambi, Vol. 5, No. 2, Jambi: Universitas Jambi, 2014, hlm.95.
[6] Barda Nawawi Arief, *Tindak Pidana Mayantara,* Raja Grafindo Persada, Jakarta, 2006, hlm. 1.

Cybercrime apabila kita terjemahkan kedalam bahasa Indonesia maka artinya kejahatan siber. Arti kata siber sendiri secara umum dikenal sebagai perangkat komputer, internet, teknologi informasi komunikasi dan berbagai hal yang berhubungan dengan komputer. Kejahatan merupakan perbuatan tertentu yang dilarang yang bertentangan dengan hukum dan diancam pidana *(criminal act).* Menurut Simons kejahatan adalah kelakuan/handelin yang diancam pidana yang bersifat melawan hukum yang berhubungan dengan kesalahan dan dilakukan oleh orang yang mampu bertanggung jawab.[7]

Cybercrime adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime* merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet.

Pengertian lainnya mengenai *cybercrime* adalah kejahatan berbasis teknologi telematika yang selanjutnya disebut sebagai kejahatan telematika dalam berbagai sumber sering disebut dengan istilah : Penyalahgunaan Komputer atau Kejahatan Komputer *(computer crime; computer related crime; computerassisted crime),* Kejahatan Mayantara *(cybercrime),* Kejahatan Komputer *(computer cyber)*.[8]

---

[7] Harum Pudjiarto, *Handout Hukum Pidana, Fakultas Hukum* Universitas Atma Jaya Yogyakarta, hlm. 9

[8] Aloysius Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika*, Penerbit Universitas Atma Jaya Yogyakarta, Yogyakarta, 2010, hlm. 1

Pengertian *cybercrime* menurut Widodo adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara material maupun melawan hukum secara formal. Widodo menjelaskan *cybercrime* dapat dibedakan menjadi 2 (dua) kategori, yaitu *cybercrime* dalam arti sempit dan *cybercrime* dalam arti luas. *Cybercrime* dalam arti sempit adalah kejahatan terhadap sistem komputer, sedangkan dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan komputer.[9]

Batasan atau definisi dari kejahatan komputer juga diberikan oleh Andi Hamzah, bahwa "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal".[10] Dari pengertian yang diberikan oleh Andi Hamzah dapat disimpulkan bahwa beliau memperluas pengertian kejahatan komputer, yaitu segala aktivitas tidak sah yang memanfaatkan komputer untuk tindak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau illegal merupakan suatu kejahatan.

2. Pengaturan *Cybercrime* Dalam Sistem Hukum di Indonesia

Cybercrime atau kejahatan dunia maya dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan

---

[9] Widodo, *Sistem Pemidanaan dalam Cybercrime,* Laksbang Meditama, Yogyakarta, 2009, hlm. 24.
[10] Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer,* Sinar Grafika, Jakarta, 1989, hlm. 26.

dengan teknologi informasi, hal ini sejalan dengan pengertian yang diberikan oleh Donn B. Parker yang memberikan definisi mengenai penyalahgunaan komputer

:"*Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain*", dan diterjemahkan oleh Andi Hamzah sebagai "penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan.[11]

Adapun Pengaturan Tindak Pidana *Cybercrime* di Indonesia :

a. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Dalam undang-undang tersebut terdapat beberapa pasal yang mengatur perbuatan yang dilarang yang termasuk tindak pidana *cybercrime.* Sebelum ada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini yang digunakan untuk mengancam pidana bagi perbuatan yang dikategorikan dalam tindak pidana *cybercrime.* Namun undangundang ini hanya mengatur beberapa tindak pidana yang termasuk tindak pidana *cybercrime* yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomudir tindak-tindak pidana yang berkaitan dengan komputer.

"Pasal 22 yang berbunyi: "Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi'' :

1) Akses ke jaringan telekomunikasi; dan atau
2) Akses ke jasa telekomunikasi; dan atau
3) Akses ke jaringan telekomunikasi khusus."

---

[11] Donn B. Parker, *Crime by Computer*, 1976, Hlm.12, Andi Hamzah, *Hukum Pidana yang berkaitan dengan komputer*, Sinar Grafika Offset 1993, hlm. 18

"Pasal 38 yang berbunyi : "Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi"

"Pasal 40 yang berbunyi : "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun"

Bentuk-bentuk tindak pidana *cybercrime* dalam Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi adalah Akses Ilegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi. Hal ini merujuk pada pengertian *cybercrime* yang diberikan oleh Konferensi PBB yang menyatakan *cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer atau jaringan komputer, baik pada sistem keamnannya. Telekomunikasi merupakan salah satu bentuk jaringan dan sistem komputer sehingga perbuatan yang dilarang dalam pasal pasal tersebut dapat dikategorikan menjadi tindak pidana *cybercrime.*

b. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik diundangkan pada tanggal 23 April 2008. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik memuat dan mengakomodir tentang pengelolaan informasi dan transaksi elektronik untuk pembangunan, dan juga sebagai antisipasi atau payung hukum dari resiko buruk jika

terdapat penyalahgunaan kemajuan teknologi informasi dan transaksi elektronik yang dapat merugikan kepentingan hukum baik bagi orang pribadi, masyarakat ataupun negara yang menggunakan alat teknologi atau dengan kata lain yang dapat disebut dengan tindak pidana *cybercrime.* Pengaturan *Cybercrime* dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Adapun pasal-pasal yang mengatur tindak pidana *cybercrime* dalam undang - undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah sebagai berikut :

Pasal	Materi
Pasal 27 ayat (1)	Dengan sengaja atau tanpa hak mendistribusikan dan/ atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
Psl 27 ayat (2)	Dengan sengaja tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
Psl 27 ayat (3)	Tanpa hak mendistribusikan dan/atau mentransmisikn dan/atau membuat dapat diaksesnya Informasi Elektro nik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik

Psl 27 ayat (4)	Tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman
Psl 28 ayat (1)	Tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik
Psl 28 ayat (2)	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	Tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi
Pasal 30 ayat (1)	Tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun
Pasal 30 ayat (2)	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
Pasal 30 ayat (3)	Tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.
Pasal 32 ayat (1)	Tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan trans-misi, merusak, menghilangkan, memindahkan,menye mbunyikan suatu Informasi Elektronik dan/atau Doku men Elektronik milik Orang lain atau milik publik.
Pasal 32 ayat (2)	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
Pasal 32 ayat (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	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 ayat (1)	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 me -mfasilitasi 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.
Pasal 34 ayat (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	Tanpa hak atau melawan hukum melakukan manipula-si, 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	Tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain.
Pasal 37	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.

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang *cybercrime* dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu.

c. Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik merupakan bentuk dari perubahan Undang- undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi

Elektronik. Namun terkait dengan bentuk-bentuk dari tindak pidana *cybercrime* yang diatur tidak ada perubahan, sehingga segala bentuk tindak pidana *cybercrime* masih sama halnya dengan yang diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Perbedaan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah sebagai berikut :

N0	UU No 11 Tahun 2008 tentang ITE	UU No 19 tahun 2016 tentang Perubahan UU No 11 Tahun 2008 tentang ITE
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. Rumusan pasal mengenai bentuk-bentuk tindak pidana Rumusan bentuk-b.
2	Rumusan pasal mengenai bentuk-bentuk tindak pidana	Rumusan bentuk-bentuk tindak pidana ITE masih tetap sama dengan UU sebelumnya tidak ada penambahan

		rumusan pasal mengenai perbuatan yang dilarang hanya terdapat perubahan dalam pasal 31.
3	Tidak adanya penjelasan menge n-ai Pasal 5 tentang alat bukti elektronik	Dirubah dengan penambahan penjelasan dalam Pasal 5.
4	Tidak adanya kewajiban penyel enggara 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 pengeledahan, penyitaan barang bukti yakni mutlak harus melalui izin pengadilan	Adanya perubahan dalam penggeledahan dan penyitaan barang bukti elektronk dilakukan sesuai dengan ketentuan hukum acara pidana dalam KUHAP.

3. Karakteristik dan Jenis-Jenis *Cybercrime* .

Berdasarkan beberapa literatur dan prakteknya, *cybercrime* memiliki beberapa karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain[12] :

a. Perbuatan yang dilakukan secara illegal, tanpa hak tersebut terjadi di ruang/wilayah maya *(cyber space),*sehingga sulit dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.
c. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
e. Perbuatan tersebut sering kali dilakukan secara transnasional/ melintasi batas negara.

Jenis-jenis Tindak Pidana *Cybercrime* [13]

a. *Unauthorized access to computer system and srvice,* ialah kejahatan yang dilakukan ke dalam sesuatu sistem jaringan komputer secara tidak legal, tanpa izin, ataupun tanpa pengetahuan dari *owner* sistem jaringan komputer yang dimasukinya. Biasanyan pelaku kejahatan *(hacker)* melakukannya dengan maksud sabotase maupun pencurian data penting serta rahasia. Tetapi ada pula

---

[12] Ari Jualino Gema, http://www.hukum*online*.com/berita/baca/hal229/*cybercrime*-sebuah-fenomenadi-dunia-maya, diakses 31 Mei 2021, pukul 09.00 WIB.
[13] Maskun*, Kejahatan Siber;cybercrime Suatu Pengantar*. Jakarta: Kencana,2013 hlm. 51-54

yang melakukannya sebab merasa tertantang buat mencoba keahliannya menembus sesuatu sistem yang mempunyai tingkatan keamanan tinggi.

b. *Illegal contents,* ialah kejahatan dengan memasukkan informasi ataupun data ke internet tentang suatu hal yang tidak benar, tidak etis, serta dianggap melanggar hukum dan menganggu ketertiban umum contohnya :

- Pemuatan kabar bohong ataupun fitnah yang hendak menghancurkan martabat ataupun harga diri pihak lain.
- Pemuatan hal- hal yang berhubungan dengan pornografi.
- Pemuatan sesuatu data yang merupakan rahasia negara, agitasi, dan propaganda buat melawan pemerintah yang legal, serta sebagainya.

c. *Data forger,* yakni kejahatan dengan memasukkan informasi pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* lewat internet, Kejahatan ini umumnya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi salah ketik yang pada akhirnya bakal mengguntungkan pelaku.

d. *Cyber espionage,* ialah kejahatan yang menggunakan jaringan internet untuk melakukan aktivitas mata- mata terhadap pihak lain, dengan merambah sistem aringan komputer*(computer network system)* pihak target. Kejahatan ini umumnya ditujukan terhadap saiangan bisnis yang dokumen maupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi.

e. *Cyber sabatage and extartio*n, ialah kejahatan yang dilakukan dengan membuat gannguan, perusakan ataupun penghancuran terhadap suatu informasi, program komputer ataupun sistem jarimgan komputer yang terhubung dengan internet.

Biasanya kejahatan ini dilakukan dengan menyusupkan sesuatu *logic bomb*, virus komputer aataupun sesuatu program tertentu, sehingga informasi, program komputer ataupun sistem jaringan komputer tidak bisa digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana dikehendaki oleh pelaku. Dalam sebagian permasalahan setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki informasi, program komputer, pastinya dengan bayaran tertentu.

f. *Offence against intellectual property*, ialah kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dipunyai seorang di internet. Sebagai contoh yaitu peniruan tampilan *web page* milik orang lain secara ilegal, penyiaran suatu data di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

g. *Infrigements of privacy*, ialah kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat individu serta rahasia. Kejahatan ini umumnya diperuntukan terhadap keterangan pribadi seorang yang tersimpan pada formulir informasi pribadi seorang yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, hingga bisa merugikan secara material ataupun imaterial, seperti no. kartu kredit, no. PIN ATM, keterangan tentang cacat ataupun penyakit tersembunyi, dan sebagainya.

B. Tinjauan Umum Tentang Tindak Pidana *Carding*

1. Pengertian Tindak Pidana *Carding*

Kejahatan *carding* adalah suatu kejahatan dimana komputer sebagai alat untuk melakukan kejahatan *carding* tersebut, dimana tindak pidana *carding* ini merupakan salah satu jenis kejahatan yang dikenal dengan istilah *cybercrime. Carding*

merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet[14].

Carding adalah pembobolan kartu kredit ataupun digital kredit dan digunakan untuk membeli dengan menggunakan nomor dan identitas kartu kredit orang lain yang dapat diperoleh secara ilegal, biasanya mencuri data di internet *carding* dapat disebut sebagai salah satu tindakan kriminal atau kejahatan yang dilakukan secara *online.*

Istilah *Carding* sering dihubungkan dengan suatu aktivitas kartu kredit seperti contohnya pada transaksi *e-commerce*. Pengertian dari *Carding* itu sendiri adalah suatu bentuk kejahatan yang menggunakan kartu kredit orang lain untuk dibelanjakan tanpa sepengetahuan pemiliknya[15].

Menurut Indradi berpendapat bahwa *carding* adalah penipuan kartu kredit bila pelaku mengetahui nomor kartu kredit seseorang yang masih berlaku,maka pelaku dapat membeli barang secara *online* yang tagihannya dialamatkan pada pemilik asli kartu kredit tersebut, sedangkan pelakunya dinamakan *carder.*[16] *Carder* adalah pelaku atau orang yang bisa mempelajari, menganalisis, memodifikasi, meretas dan menerobos masuk kedalam komputer dan jaringan komputer yang aman maupun tidak aman, baik untuk keuntungan atau dimotivasi oleh tantangan.

Carding merupakan salah satu bentuk pembobolan *(theft*) dan kecurangan *(fraud)* di dunia internet yang dilakukan oleh pelakunya yang dinamakan *carder* dengan

---

[14] Dodo Zaenal Abidin, *Kejahatan Dalam Teknologi Informasi Dan Komunikasi*, Jurnal Ilmiah Media Processor, Volume 10, Nomor 2, Oktober, 2015.

[15] Endah Lestari, Johanes Arif,*Tinjauan Yuridis Kejahatan Penggunaan Kartu Kredit di Indonesia,* Jurnal Hukum, Volume XVIII, Nomor 18, April 2010, hal 1.

[16] Mehda Zuraida, *Credit card* Fraud *(Carding) dan Dampaknya Terhadap Perdagangan Luar NegeriIndonesia* , Jurnal Analisis Hubungan Internasional, Volume 4, Nomor 1, Maret, 2015, hlm. 1631

menggunakan kartu kredit curian atau kartu kredit palsu yang dibuat sendiri. Tujuannya yaitu untuk membeli barang secara tidak sah atau menarik dana secara tidak sah dari suatu rekening bank milik orang lain.[17]

2. Perkembangan Tindak Pidana *Carding* di Indonesia

Cybercrime sebagai fenomena hukum seiring dengan perkembangan tekhnologi informasi menjelma menjadi tindak pidana yang mengkhawatirkan masyarakat di dunia, termasuk juga Indonesia. Kekhawatiran tentang tindak pidana ini dapat dirasakan dalam berbagai aspek kehidupan.Salah satu tindak pidana yang diakibatkan oleh perkembangan tekhologi adalah tindak pidana menggunakan kartu kredit palsu *(Carding)*. Tindak pidana menggunakan kartu kredit palsu *(Carding)* adalah tindak pidana dengan menggunakan tekhnologi komputer untuk melakukan transaksi dengan menggunakan kartu kredit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.

Indonesia dalam kejahatan dunia maya (menggunakan internet) menempati urutan *runer-up* dunia setelah Ukraina yang sebelumnya menduduki peringkat pertama.[18] Kasus semacam ini banyak dilakukan oleh *carder* dari Yogyakarta dan berbagai kota besar lainnya di Indonesia, yang pada umumnya berstatus sebagai mahasiswa. Perbuatan *carder* yang dilakukan di Indonesia sudah bebas dan transparan,mulai dari bertukar nomor kartu kredit di server Dalnet IRC sampai mempunyai situs internet khusus untuk saling bertukar nomor kartu kredit yang didapat.

---

[17] Abdul Wahid dan Labib Mohammad, *Kejahatan Mayantara (Cyber Crime),* Bandung: RefikaAditama, 2010, hlm 7

[18] https://news.rakyatku.com/read/135627/2019/01/15/Indonesia-pelaku-kejahatan-*carding* terbanyak-kedua-di-dunia, Diakses pada tanggal 25 Juni 2021, pukul 15.00 WIB.

Banyak *carder* Indonesia yang sudah menjadikan aktivitas ini sebagai sebuah profesi yang dilatarbelakangi oleh motif ekonomi yaitu bagaimana mendapatkan keuntungan secara ilegal. Banyak dari mereka yang melakukan aktivitas diwarung-warung internet (warnet) untuk mempersulit pelacakan keberadaanmereka. Hal ini dilakukan supaya mereka dapat dengan cepat berpindah-pindah tempat. Hanya orang bodoh yang melakukan *carding* dengan menggunakan *dial-up* dari rumahnya karena akan berdampak buruk pada kejahatan yang dilakukan.

3. Pihak-Pihak yang Terkait Dalam Tindak Pidana *Carding*

Dalam kejahatan *Carding* tentu tidak terlepas dari pihak-pihak yang terkait dalam pelaku *carding*. Berikut ini adalah pihak-pihak yang terlibat dalam kejahatan *carding:*

a. Carder

Carder merupakan pelaku dari *carding*. Carder memakai e-mail,*banner* ataupun *pop-up window* untuk menipu netter ke suatu situs website palsu, dimana netter diminta untuk membagikan informasi pribadinya. Teknik umum yang kerap digunakan oleh para *carder* dalam aksi pencurian merupakan membuat web ataupun e-mail palsu atau disebut juga *phising* dengan tujuan mendapatkan data nasabah seperti no rekening, PIN *(Personal Identification Number),* ataupun *password.* Pelaku kemudian melakukan konfigurasi PIN ataupun *password* setelah mendapatkan informasi dari nasabah, sehingga bisa mengambil dana dari nasabah tersebut. Sasaran *carder* ialah pengguna layanan internet *banking* ataupun situs- situs iklan, jejaring sosial, *online shopping* serta sejenisnya yang ceroboh dan tidak cermat dalam melakukan transaksi secara *online* lewat web internet. *Carder* mengirimkan beberapa e-mail ke sasaran target dengan tujuan untuk meng up-date ataupun mengganti user ID serta PIN

nasabah melalui internet. E-mail tersebut terlihat seperti dikirim dari pihak resmi, sehingga nasabah kerapkali tidak menyadari jika sebenarnya lagi ditipu. Pelaku *carding* mempergunakan sarana internet dalam mengembangkan teknologi informasi tersebut dengan tujuan yakni menimbulkan rusaknya lalu lintas mayantara *(cyberspace)* demi terwujudnya tujuan tertentu antara lain keuntungan pelaku dengan merugikan orang lain disamping yang membuat, atau pun menerima informasi tersebut.

b. Netter

Netter adalah pengguna internet, dalam hal ini adalah penerima email (nasabah sebuah bank) yang dikirimkan oleh para *carder.*

c. Cracker

*Cracke*r adalah sebutan untuk orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang dimasuki seperti pencurian data, penghapusan, penipuan, dan banyak yang lainnya.

d. Bank

Bank adalah badan hukum yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkan kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak. Bank juga merupakan pihak yang menerbitkan kartu kredit/debit, dan sebagai pihak penyelenggara mengenai transaksi *online, ecommerce*, *internet banking*, dan lain-lain

4. Undang-Undang yang Mengatur *Carding*

Berbicara tindak pidana *carding* tidak terlepas dari suatu kejahatan dimana komputer sebagai alat untuk melakukan kejahatan *carding* tersebut, dimana tindak pidana

carding ini merupakan salah satu jenis kejahatan yang dikenal dengan istilah *cybercrime.* Perkembangan teknologi dengan berbagai bentuk kecanggihan informasi, komunikasi dan transportasi membuat modus kejahatan semakin marak dilakukan oleh pelaku-pelaku kejahatan, diantaranya kejahatan yang menggunakan komputer dan internet sebagai alat bantunya untuk melakukan kejahatan di bidang kartu kredit atau yang dikenal dengan tindak pidana *carding.*

Kebijakan pengaturan tindak pidana *carding* terdapat di dalam Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu yang berkaitan dengan perbuatan menggunakan dan atau mengakses kartu kredit orang lain secara tanpa hak. Ketentuan Pasal 51 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik hanya dapat menjangkau pelanggaran pada tahapan *card embossing and delivery (courier/recipient or customer)* dan *usage.* Tidak semua modus operandi dalam tahapan tersebut dapat terjangkau, karena ketentuan Pasal 51 jo Pasal 34 UndangUndang Nomor 11 Tahun 2008 hanya mengatur perbuatan yang dilakukan oleh orang yang menggunakan kartu kredit tetapi tidak termasuk pedagang atau pengelola yang juga dapat menjadi pelaku tindak pidana *carding.*

Pasal 51 Undang-Undang Nomor 11 Tahun 2008 menyebutkan bahwa : "Setiap orang dengan sengaja dan melawan hukum melanggar hukum melanggar ketentuan sebagaimana dimaksud dalam Pasal 34 ayat (1), Pasal 34 ayat (2), Pasal 35, atau Pasal 36 ayat (1), dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau denda paling banyak Rp.2.000.000.000,- (dua milyar rupiah)".

Pasal 34 Undang-Undang Nomor 11 Tahun 2008 menyebutkan bahwa : "Setiap orang dilarang dengan sengaja dan melawan hukum : ayat (1) : Menggunakan dan atau mengakses komputer dan atau sistem elektronik secara tanpa hak dan melampaui wewenangnya dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari lembaga perbankan dan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya.

ayat (2) :

"Menggunakan dan atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan".

5. Jenis-Jenis Tindak Pidana *Carding*

Kejahatan *cybercrime* khususnya *carding* dapat dibagi dalam beberapa bentuk atau jenis kejahatan *carding* yaitu antara lain:[19]

a. *Cyber trespass* kejahatan mengakses komputer atau jaringan komputer tanpa menyalahgunakan atau merusak data.
b. *Cyber theft* merupakan kejahatan untuk mencuri informasi, uang atau sesuatu yang mempunyai nilai. Keuntungan merupakan motivasi dari pelaku melakukan *cyber theft*.
c. *Cyber fraud* penipuan melalui internet berbeda dengan pencurian. Dalam *cyber fraud* korban mengetahui dan secara sukarela memberikan uangnya kepada pelaku kejahatan.

[19] Sigid Suseno dan Syarif A. Barmawi, *Kebijakan Pengaturan Carding Dalam Hukum Pidana DiIndonesia*, Jurnal Sosiohumaniora, Volume 6, Nomor 3, November , 2004, hlm. 249

d. *Destructive cybercrimes* merusak atau menghancurkan data atau jaringan pelayanan. Misalnya meretas ke dalam jaringan dan menghapus data atau file program, meretas ke dalam server web dan merusak halaman web.

Menurut Indrawan ada beberapa jenis tindak pidana *carding* sebagai berikut:[20]

a. *Misus (compromise) of card data,* yaitu berupa penyalahgunaan kartu kredit yang tidak di presentasikan.
b. *Counterfeiting,* yaitu pemalsuan kartu kredit. Kartu palsu sudah diubah sedemikian rupa menyerupai kartu asli. *Carding* jenis ini dilakukan oleh perorangan sampai sindikat pemalsu kartu kredit yang memiliki jaringan luas, dana besar dan didukung oleh keahlian tertentu. Perkembangan *Counterfeiting* saat ini telah menggunakan software tertentu yang tersedia secara umum di situs-situs tertentu *(credit master,credit probe*) untuk menghasilkan nomor-nomor kartu kredit serta dengan menggunakan mesin atau terminal yang dan telepon genggam untuk mengecek keabsahan nomor-nomot tersebut.Selain itu, *counterfeiting* juga menggunakan *skimming device* yang berukuran kecil untuk mengkloning data yang tertera di *magnetikstripe* kartu kredit asli dan menggunakan peralatan-peralatan untuk meng-*intercept* jaringan telekomunikasi serta menggunakan terminal *implants*.
c. *Wire tapping,* yaitu penyadapan transaksi kartu kredit melalui jaringan komunikasi.

---

[20] Indrawan*, Sanksi Pidana Bagi Pelaku Kejahatan Carding Ditinjau Dari Hukum Positif Dan Hukum Pidana Islam,* Skripsi Sarjana Hukum, Fakultas Syariah Institut Agama Islam Negeri Surakarta, Surakarta, 2020, hlm. 32-33

d. *Phissing*, yaitu penyadapan melalui situs website agar personal data nasabah dapat dicuri

6. Modus *Carder* Dalam Melakukan *Carding*

Dalam kejahatan *Carding* modus operandi nya terus berkembang dari waktu ke waktu. Karena sebelumnya, 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 dikartu 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[21]

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 menitipkan.Tetapi umumnya chip ini harus dipasang oleh petugas yang

[21] Data di akses dari http://www.kompas.com/ Pemalsuan Kartu Kredit Semakin Merajalela, tanggal 07 Juni 2021, pukul 12:00 WIB.

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.

Beberapa modus operandi yang dapat dilakukan sesua dengan alur proses kartu kredit tersebut antara lain:[22]

a) Fraud application

Menggunakan kartu kredit asli yang diperoleh dengan aplikasi palsu.Pelaku memalsukan data pendukung dalam proses aplikasi seperti KTP, Pasport, rekening koran, Surat Keterangan Penghasilan dan lain-lain

b) Lost/stolen card

Menggunakan kartu kredit asli hasil curian atau hilang. Pada waktu melakukan transaksi pelaku menandatangan / dan meniru tanda tangan pada kartu kredit atau tanda tangan pemegang kartu yang sah. Transaksi dilakukan di bawah floor limit agar tidak perlu dilakukan otorisasi.

c) *Totally counterfeited*

Menggunakan kartu kredit yang seluruhnya palsu. Pelaku mencetakkartu tiruan dengan menggunakan data nomor dan pemegang kartu yang masih berlaku dengan melakukan mengatur ulang sandi dan data baru *(reembossed dan reencoded)*

d) Record of charge (Roc) pumping

---

[22] Sigid Suseno Dan Syarif A. Barmawi, *Op. Cit* 254-255

Penggandaan sales draft oleh *merchant* (pedagang). Sales draft yang satu tidak ditandatang oleh pemegang kartu yang sah dan diserahkan kepada *merchant* lain untuk disi dengan data transaksi fiktif

e) Altered amount

Mengubah nila transaksi pada sales draft oleh *merchant* (pedagang).

f) Telephone/mail ordered

Memesan barang melalui telepon atau surat dengan menggunakan kartu kredit orang lain yang sudah diketahu nama dan nomornya.

g) Mengubah program Electronic Data/Draft Capture (EDC)

Mengubah dan merusak program pada alat otorisas *(electronicdata/draft capture/EDC)* milik pengelola oleh *merchant* (pedagang).

h) Fictius merchant

Pelaku berpura-pura menjadi pedagang dengan mengajukan aplikasi disertai dengan data-data palsu

C. Tinjauan Umum Pertanggungjawaban Pidana

1. Pengertian Pertanggunggjawaban Pidana

Pertanggungjawaban pidana dalam istilah asing disebut dengan *teorekenbaarddheid atau criminal responsibility* yang menjurus kepada pemidanaan pelaku dengan maksud untuk menentukan apakah seseorang terdakwa atau tersangka dipertanggungjawabkan atau suatu tindakan pidana terjadi atau tidak.[23]

[23] H. A. Zainal Abidin Farid, *Hukum Pidana 1*, Sinar Greafika, Jakarta, 2010, hlm 222

Pertanggungjawaban pidana adalah pertanggungjawaban orang terhadap tindak pidana yang dilakukannya.

Tegasnya yang dipertanggungjawabkan orang itu adalah tindak pidana yang dilakukannya. Dengan demikan, terjadinya pertanggungjawaban pidana karena telah ada tindak pidana yang dilakukan oleh seseorang. Pertanggungjawaban pidana pada hakikatnya merupakan suatu mekanisme yang dibangun oleh hukum pidana untuk mereaksi terhadap pelanggaran atas „kesepakatan menolak" suatu pebuatan tertentu.[24] Pertanggungjawaban pidana menjurus kepada pemidanaan petindak, jika telah melakukan suatu tindak pidana apabila telah melakukan suatu tindak pidana dan memenuhi unsur-unsurnya yang telah ditentukan dalam undang-undang. Berdasarkan dari sudut pandang terjadi suatu tindakan yang terlarang (diharuskan), seseorang akan dipertanggungjawabkan atas tindakan-tindakan tersebut apabila tindakan tersebut bersifat melawan hukum untuk itu.

2. **Unsur-Unsur Pertanggungjawaban Pidana**

Pertanggungjawaban adalah bentuk untuk menenutukan apakah seseorang akan dilepas atau dipidana atas tindak pidana yang telah terjadi, dalam hal ini untk mengatakan bahwa seseornag memiliki aspek pertanggung jawaban pidana maka dalam hal itu terdapat beberapa unsur yang harus terpenuhi untuk menyatakan bahwa seseornag tersebut dapat dimintakan pertanggungjawaban. Unsur-unsur tersebut ialah:

[24] Chairul Huda, *Op. Cit* hlm 70

a. Unsur kesalahan

Kesalahan yang dalam bahasa asing disebut dengan schuld adalah keadaan psikologi seseorang yang berhubungan dengan perbuatan yang ia lakukan yang sedemikian rupa sehingga berdasarkan keadaan tersebut perbuatan tersebut pelaku dapat dicela atas perbuatannya.[25] Kesalahan sebagai unsur pertanggungjawaban dinilai setelah terpenuhinya semua unsur tindak pidana atau terbuktinya tindak pidana, yang menjadi parameter untuk menilai adanya kesalahan sebagai unsur pertanggungjawaban pidana adalah tujuan, atau maksud dibentuknya norma hukum dalam perudang-undangan dalam hubungannya dengan tindak pidana yang telah dilakukan oleh pembuat.

b. Kemampuan bertanggungjawab

Kemampuan bertanggungjawab selalu berhubungan dengan keadaan psikis pembuat. Kemapuan bertanggungjawab ini selalu dihubungkan dengan pertanggungjawaban pidana, hal ini yang menjadikan kemampuan bertanggungja-waban menjadi salah satu unsur pertanggungjawaban pidana. Kemampuan bertanggung jawab merupakan dasar untuk menentukan pemidanaan kepada pembuat. Kemampuan bertanggung jawab ini harus dibuktikan ada tidaknya oleh hakim, karena apabila seseorang terbukti tidak memiliki kemampuan bertanggung jawab hal ini menjadi dasar tidak dipertanggungjawabkannya pembuat, artinya pembuat perbuatan tidka dapat dipidana atas suatu kejadian tindak pidana.

c. Unsur kesengajaan (*dolus)* dan unsur kealapaan *(culpa)*

Dalam tindak pidana kebanyakan di Indonesia memiliki unsur kesengajaan atau *opzettelijik* bukan unsur *culpa.* Hal ini berkaitan bahwa orang yang lebih pantas

[25] Moeljalento, *Asas-Asas Hukum Pidana, Edisi revisi,* Renika Cipta, Jakarta, 2008, hlm 25

mendapatkan hukuman adalah orang yang melakukan hal tersebut atau melakukan tindak pidana dengan unsur kesengajan. Kesengajan telah berkembang dalam yurisprudensi dan doktrin sehingga umumnya telah diterima beberapa bentuk kesengajaan, yaitu :

i. Sengaja sebagai maksud *(opzet als oogemark)*

ii. Sengaja dengan kesadaran tentang kepastian *(opzet met bewustheid van zakerheid of noodzakelijkheid)*

iii. Sengaja dengan kesadaran dengan kemungkinan terjadi *(opzet met waarschijkheidbewustzjin)*

Kelalaian *(culpa)* Undang-undang tidak memberikan definisi yang dimaksud dengan kelalaian. Tetapi hal tersebut dapat dilihat dalam MvT *(Memori van Toelichting)* yang menyatakan bahwa kelalaian (culpa) terletak antara sengaja dan kebetulan.

d. Tidak adanya alasan pemaaf

Dalam keadaan tertentu seseorang pelaku tindak pidana, tidak dapat melakukan tindakan lain selain melakukan perbuatan tindak pidana, meskipun hal itu tidak di inginkan. Sehingga dengan perbuatan tersebut pelaku nya harus menghadi jalur hukum. Hal itu tidak dihindari oleh pelaku meskipun hal itu tidak diinginkan oleh dirinya sendiri. Hal itu dilakukan oleh seseorang karena faktor-faktor dari luar dirinya.[26] Dalam doktrin hukum pidana alasan pemaaf dan alasan pembenar, alasan

[26] Chairul Huda*, Dari tiada Pidana tanpa Kesalahan Menuju Tiada Pertanggungjawaban Pidana Tanpa Kesalahan,* Kencana, Jakarta, 2006, hlm-116

pembenar adalah suatu alasan yang menghapus sifat melawan hukumnya suatu perbuatan. Alasan pembenar dan alasan Dalam hukum pidana yang termasuk alasan pembenar seperti keadaaan darurat, pembelaan terpaksa, Menjalankan peraturan perundang-undangan, menjalankan perintah jabatan yang sah. Keadaan darurat merupakan salah satu alasan pembenar, yaitu suatu alsan karena seseorang menghadapi dilema situasi untuk memilih suatu tindakan. Dalam hukum pidana yang dimaksud dengan alasan pemaaf adalah hukum pidana adalah tidak mampu bertanggungjawab, daya paksa, pembelaan terpaksa melampaui batas,mengenai ketidak mampuan bertanggung jawab telah dijabarkan sebelumnya, hal ini berkaitan dengan keadaan seseorang dapat atau tidak diri seorang pelaku tersebut melakukan pertanggungjawaban mengenai suatu hal yang telah diperbuat.

BAB III

METODOLOGI PENELITIAN

A. Ruang Lingkup Penelitian

Ruang lingkup penelitian adalah dimaksud untuk membatasi permasalahan yang akan dibahas dalam penelitian ini. Adapun ruang lingkup dalam penelitian ini adalah Bagaimana pertanggungjawaban pidana terhadap pelaku *cybercrime* dalam pembobolan kartu kredit (*carding)* dalam putusan nomor 1229/Pid.Sus/2020/ PN Mks dan Bagaimana pertimbangan hakim terhadap *cybercrime* dalam pembobolan kartu kredit (*carding)* dalam putusan nomor 1229/Pid.Sus/2020/PN Mks.

B. Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah jenis penelitian hukum Normatif. Penelitian hukum normatif *(Normatif law research)* adalah metode yang dilakukan dengan cara meneliti bahan-bahan pustaka yaitu, buku, jurnal,artikel-artikel resmi,menelusuri doktrin-doktrin dan teori hukum dari berbagai literatur dan peraturan perundang-undangan yang berlaku dan berhubungan dengan pokok pembahasan permasalahan.

C. Metode Pendekatan Masalah

Ada beberapa metode pendekatan masalah yang digunakan dalam penelitian penulisan ini antara lain yaitu :

1. Pendekatan Perundang-undangan *(Statue Approach)* yakni pendekatan yang dilakukan dengan cara menelaah semua peraturan perundangan dan regulasi yang bersangkut paut dengan isu hukum yang ditangani.[27]

[27] Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi,* Kencana Premada Media Group, Jakarta 2005, Hal 131

2. Pedekatan Kasus *(Case Approach)* yakni pendekatan yang dilakukan dengan isu yang dihadapi telah menjadi putusan pengadilan yang telah mempunyai kekuatan hukum tetap, yaitu putusan nomor 1229/Pid.Sus/2020/PN Mks.
3. Pendekatan Konseptual yakni pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum.

D. Sumber Bahan Hukum

Adapun dalam penelitian ini, memakai 2 (dua) bahan hukum yang digunakan dalam penelitian penulisan yaitu metode penelitian hukum normatif. Metode penelitian hukum normatif terdiri dari :

1. Bahan Hukum Primer *(Primary Law Ma*terial) merupakan bahan hukum yang bersifat autoritatif, artinya mempunyai otoritas. [28] Bahan hukum primer dalam penelitian ini yaitu terdiri dari peraturan perundang-undangan yang memiliki kaitan dengan permasalahan yang dibahas dalam penelitian ini yaitu :
   a) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
   b) Undang-Undang No. 8 Tahun 1981 Tentang Kitab Undang-Undang Acara Pidana.
2. Bahan Hukum Sekunder *(Secondary Law Material)* adalah buku-buku hukum, termasuk skripsi, tesis, dan disertai hukum dan jurnal-jurnal hukum.[29] Dalam penelitian ini bahan hukum sekunder yang dipakai adalah buku-buku hukum, jurnal-jurnal hukum, dan kamus hukum.

E. Metode Penelitian

[28] *Ibid,* Hal 181
[29] *Ibid,* Hal 195.

Metode penelitian adalah ilmu yang mempelajari tentang tata cara atau prosedur untuk melakukan seluruh aktivitas atau kegiatan penelitian. Penelitian ini menggunakan metode analisis yang dilakukan untuk mengumpulkan data dengan cara studi kepustakaan. Bahan hukum primer peraturan perundang-undangan yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Adapun metode penelitian bahan hukum sekunder berupa publikasi tentang hukum dari berbagai literatur yang berakaitan dengan masalah yang diteliti serta mengutip beberapa pendapat sarjana kemudian menyusunnya secara sistematis untuk menjawab permasalahan pada Putusan Nomor 1229/Pid.Sus/2020 Mks.

F. Analisis Bahan Hukum

Bahan yang diperoleh dianalisis secara normatif kualitatif, yaitu analisis Putusan Nomor 1229/Pid.Sus/2020 Mks tentang Kejahatan *Cybercrime* Dalam Pembobolan Kartu Kredit (*Carding)*, kemudian dilakukan pembahasan dan penafsiran yang
pada akhirnya ditarik kesimpulan tentang masalah-masalah yang ada