BAB III

ALTERNATIF PENGATURAN CARDING KE DALAM IUS CONSTITUENDUM

3.1. Kelemahan Undang-Undang Informasi Dan Transaksi Elektronik

Negara Indonesia telah mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yaitu kebijakan yang berhubungan dengan hukum teknologi informasi. Tujuan utama pengesahan produk hukum ini adalah memanfaatkan teknologi informasi, media, dan komunikasi untuk memberikan rasa aman dan memberikan kepastian hukum agar dapat berkembang dengan optimal. Selain itu UU ITE disahkan untuk kesejahteraan sosial (*social welfare*) dan untuk melindungi masyarakat (*social defence*). Tetapi dalam pelaksanaannya UU ITE belum dapat menurunkan angka kejahatan siber secara signifikan di Indonesia.

Evaluasi terhadap kebijakan di dunia maya tetap diperlukan sekiranya ada kelemahan dalam kebijakan tersebut dan semakin berkembangnya modus kejahatan setiap harinya. Evaluasi tetap perlu dilakukan mengingat adanya keterkaitan antara kebijakan penegakan hukum (*law enforcement policy*), formulasi perundang-undangan (*legislative policy*) dan kebijakan pemberantasan/penanggulangan kejahatan (*criminal policy*). Kebijakan penegakan

hukum pidana dan kebijakan penanggulangan kejahatan dipengaruhi oleh kelemahan kebijakan formulasi hukum pidana.[47]

Karakteristik dari kejahatan siber adalah bisa terjadi antar negara (*transnasional*). Berhubungan dengan yuridiksi akan terdapat masalah tersendiri dengan adanya ketentuan internasional dari kejahatan *carding*. Yuridiksi merupakan hukum kekuasaan negara terhadap warga negara, benda atau peristiwa (hukum). Prinsip dasar kedaulatan negara, prinsip tidak ikut campur tangan negara lain, dan kesamaan derajat negara merupakan cerminan utama dari yuridiksi. Maka dari itu, suatu negara tidak dapat melakukan tindakan yang melewati kedaulatannya (*act of sovereignty*) di wilayah negara lain, kecuali dengan mendapatkan persetujuan dari negara itu sendiri.[48]

Pengertian yuridiksi secara konvensional adalah tentang geografis suatu negara sedangkan untuk komunikasi multimedia bersifat internasional, multi yuridiksi, tanpa batas sehingga sulit untuk memastikan yuridiksi sebagai pemanfaatan teknologi informasi yang berlaku di suatu negara dalam hal komunikasi multimedia.[49]

Pengaturan mengenai yuridiksi merupakan hal penting dalam penanganan kasus *cybercrime*, perlu dipikirkan bentuk yuridiksi yang mampu menjangkau

---

[47] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Prenada Media Group, Jakarta, 2007, hlm. 214-215.

[48] Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, 1992, hlm. 30.

[49] Tien S. Saefulah, *Juridiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace*, artikel dalam Cyberlaw:Suatu Pengantar, Pusat Studi Cyberlaw Fakultas Hukum UNPAD, ELIPS, 2002, hlm. 96.

kejahatan siber. Terkait tindak pidana *cybercrime* dibutuhkan prinsip-prinsip yuridiksi yang jelas berasal dari hukum internasional. Dalam hukum internasional diakui prinsip-prinsip dalam kegiatan dunia maya oleh setiap negara, yang akan memberikan kemudahan bagi negara-negara untuk menjalin kerjasama dengan tujuan membentuk harmonisasi peraturan-peraturan pidana untuk menanggulangi kasus *cybercrime*.[50]

Masalah yuridiksi berhubungan dengan kecakapan suatu forum untuk mengadili suatu kasus (*adjudicate jurisdiction*). Teori yang digunakan untuk yuridiksi dunia maya yaitu :

a. *The theory of uploader and downloader*. *Uploader* adalah pemberi informasi dan *downloader* adalah penerima transaksi elektronik.
b. *The law of the server*. Ditentukan dengan cara menggunakan *server* dimana *webpages* secara nyata berada, dimana *server* tersebut tercatat sebagai data elektronik.
c. *The theory of international spaces*, bahwa internet dijadikan ruang tersendiri.

UU ITE telah mengatur tentang yuridiksi yang menerapkan asas universal yang dapat digunakan dan diperlukan kerjasama dengan negara-negara lain untuk memberantas kejahatan *cybercrime*. Undang-Undang Nomor 11 Tahun 2008 menganut asas *extra territorial jurisdiction* di dalam Pasal 2 yang menjelaskan tentang yuridiksi.

[50] Darrel Menthe, *Jurisdiction in Cyberspace:A Theory of International Sraces*, http://www.mtlr.org/volfour/menthe, diakses tanggal 30 Desember 2020.

Pasal 2

"Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia."

Pro dan kontra terjadi ketika disahkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. UU ITE dirasa tidak dapat menurunkan tingkat kejahatan siber. Keefektifan UU ITE masih dipertanyakan apabila dilihat dari aspek pidananya. Berdasarkan hasil penelitian, masih banyak permasalahan yang timbul dalam implentasi UU ITE yang mengandung aspek pidana. Banyak faktor-faktor tertentu yang menghambat penegakan hukum untuk kejahatan siber secara umum.

Faktor tersebut adalah tolak ukur efektifitas penerapan penegakan hukum yang saling berhubungan. Faktor penghambat tersebut adalah :

a. Peraturan perundang-undangan;

b. Penegakan hukum yang terdiri dari pihak yang membentuk dan menerapkan hukum.

Hal yang menjadi sorotan utama dalam terbentuknya Undang-Undang Nomor 11 Tahun 2008 adalah masalah asas teritorial dan pengukuran alat bukti yang sah. Meskipun masih ada masalah lain yang menjadi sorotan utama dalam Undang-Undang Nomor 11 Tahun 2008 tetapi masalah asas territorial dan

pengukuran alat bukti yang sah juga menjadi masalah yang penting dalam penanganan kasus *cybercrime*.

Dalam masalah pembuktian terhadap tindak pidana, Undang-Undang Nomor 11 Tahun 2008 telah memberikan variasi terbaru dengan adanya pengakuan terhadap *digital evidence* sebagai alat bukti yang sah dengan persyaratan tertentu yang diatur di dalam Bab III Undang-Undang Nomor 11 Tahun 2008. Hal ini sangat diperlukan mengingat kejahatan siber dilakukan dengan memanfaatkan kecanggihan teknologi dan internet. Bukti-bukti yang didapat berbeda dengan kejahatan konvensional (bukti nyata), kejahatan siber memiliki bukti tidak nyata (maya) karena kejahatan dilakukan dengan tanpa adanya saksi dan dengan menggunakan perantara komputer dan internet sebagai sarana utama untuk melakukan tindak pidana kejahatan.

Ditinjau dari substansi hukumnya, Undang-Undang Nomor 11 Tahun 2008 memiliki kelemahan pada pasal-pasal yang menyangkut tindak pidana siber, yaitu :

1. Adanya pengelompokkan perbuatan yang dilarang yang berbeda-beda dalam satu pasal. KUHP mengatur perbuatan yang dilarang secara terpisah. Salah satunya terlihat di dalam Pasal 27 Undang-Undang Nomor 11 Tahun 2008 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.

Tidak adanya penjelasan mengenai pengertian kesusilaan. Persepsi setiap orang tentang definisi kesusilaan berbeda-beda. Dengan tidak adanya penjelasan tentang kesusilaan bisa saja pengertian kesusilaan sama dengan pengertian pornografi yang dimaksud di dalam UU ITE. Di dalam UU ITE telah menyamaratakan antara kata kesusilaan dengan pornografi. Pengertian kesusilaan dan pornografi sangat berbeda jika ditelaah lebih dalam lagi. Menurut KBBI pengertian kesusilaan adalah adat istiadat yang baik; sopan santun; kesopanan; keadaban; kesusilaan. Pornografi adalah sebuah jenis tingkah laku yang secara

erotis dengan dengan media gambar atau tulisan untuk membangkitkan nafsu birahi.[51]

Pada Pasal 27 ayat (2) tidak terdapat penjelasan tentang definisi perjudian. Selain itu hanya penyelenggara pengelola perjudian yang dikenakan tindak pidana tetapi pelaku perjudian tidak dikenakan tindak pidana. Berdasarkan Pasal 27 jo Pasal 45 Undang-Undang Nomor 11 Tahun 2008, yang berarti apabila informasi elektronik dan/atau dokumen elektronik memiliki muatan perjudian seseorang hanya dapat dipidana berdasarkan ketentuan pasal ini.

Pasal 27 ayat (3) menyebutkan bahwa di dunia maya tindak pidana siber disebut dengan *cyberstalking* tetapi dalam ayat ini memiliki unsur penghinaan dan/atau pencemaran nama baik. Tetapi tidak adanya penjelasan tentang maksud dari penghinaan dan/atau pencemaran nama baik menurut siapa dan batasan dari perbuatan tersebut serta batasan unsur-unsur penghinaan dan/atau pencemaran nama baik.

Begitu juga dalam Pasal 27 ayat (4) memiliki unsur pemerasan dan/atau pengancaman. Tidak dijelaskan apa definisi dari pemerasan dan pengancaman. Dalam pasal ini pengancaman adalah janji pengancam yang terkandung dalam ancamannya.

Terdapat pula dalam satu pasal, antara ayat yang satu dengan ayat lainnya terlihat berdiri sendiri (parsial) dan tidak ada keterkaitannya sama sekali. Hal ini terdapat pada Pasal 30 Undang-Undang Nomor 11 Tahun 2008 yang berbunyi :

---

[51] Pusat Bahasa, Departemen Pendidikan Nasional, *Kamus Besar Bahasa Indonesia*, Edisi ke-3, 2008.

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun 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 apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Ketentuan Pasal 30 ayat (1) adalah seseorang hanya dapat dipidana apabila pelaku memanfaatkan komputer dan/atau sistem elektronik. Korbannya adalah pemilik komputer dan/atau sistem elektronik tersebut. Pasal tersebut menegaskan bahwa cara apapun yang dilakukan pelaku dalam mengoperasikan komputer dan/atau sistem elektronik bukanlah faktor utama pelaku untuk dapat mempertanggung jawabkan perbuatan tersebut secara pidana.

Sama halnya dengan Pasal 30 ayat (1), Pasal 30 ayat (2) juga tidak menentukan bahwa pelaku dapat diberikan pertanggung jawaban pidana harus dilakukan dengan cara tertentu dalam mengoperasikan komputer dan/atau sistem elektronik. Pasal ini mengabaikan tata cara yang digunakan pelaku dalam mengoperasikan komputer dan/atau sistem elektronik tetap dapat dituntut. Pasal

ini mengatur larangan setiap orang untuk tidak melakukan *illegal accsess* dengan cara *hacking*, *cracking* maupun *cyber trespassing*.

2. Adanya ketidak konsistenan dalam penulisan pada Pasal 31 Undang-Undang Nomor 11 Tahun 2008 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 atau 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 apapun 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.

Kesimpulan dari Pasal 31 adalah melakukan tindakan penyusupan ke sistem elektronik milik orang lain merupakan hal yang dilarang, kecuali jika tindakan penyusupan merupakan permintaan institusi penegak hukum. Penyusupan adalah tindakan melawan hukum menyimpan semua informasi orang lain yang dimiliki, yang dilakukan oleh seseorang selama tidak diketahui oleh aparat penegak hukum. Dengan demikian para aparat penegak hukum tidak dapat memperoleh bukti awal yang dibutuhkan untuk melakukan pengaduan.

3. Pasal 32 dan 34 Undang-Undang Nomor 11 Tahun 2008 yang berbunyi :

Pasal 32 :

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun 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 apapun 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 34 :

(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 tersebut terkesan ambigu karena menimbulkan kesulitan dalam hal pembuktian tindak pidana *cybercrime*. Tidak adanya kejelasan dalam membuktikan unsur-unsur tindak pidana dalam pasal tersebut.

4. Adanya pasal yang secara khusus mengatur "mengakibatkan kerugian bagi orang lain". Pada Pasal 36 yang berbunyi :

   Pasal 36

   "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."

5. Adanya pasal yang tidak memerdulikan tentang masalah yuridiksi hukum. Pada Pasal 37 yang berbunyi :

   Pasal 37

   "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 yuridiksi Indonesia."

Pasal ini dibuat agar pelaku kejahatan siber dapat dikenakan sanksi pidana sesuai dengan Undang-Undang Nomor 11 Tahun 2008, yang mana jika warga negara Indonesia atau warga negara lain yang sedang berada di Indonesia melakukan tindak kejahatan berupa penipuan maupun pencurian yang terjadi di dunia maya dengan memakai secara illegal *server* yang ada di negara lain. Aturan yang termuat dalam Pasal 27 sampai dengan Pasal 34

belum memiliki standar yang sama dengan negara lain. Jadi Pasal 37 mengalami konflik yuridiksi.

6. Kandungan penjelasan pasal yang kurang sesuai dengan pasal yang dijelaskan.

   Penjelasan Pasal 30 ayat (2) Undang-Undang Nomor 11 Tahun 2008 :

   "Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan :

   a. Melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau
   b. Sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

Penjelasan tersebut di atas tidak sesuai untuk menjelaskan Pasal 30 ayat (2). Penjelasan pasal ini lebih cocok untuk menjelaskan Pasal 32 ayat (2) yang berbunyi :

Pasal 32 ayat (2)

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak."

7. Pembatasan dalam hak kebebasan berekspresi, mengutarakan pendapat dan menghambat kreatifitas masyarakat dalam penggunaan internet. Terutama dalam Pasal 27 ayat (1), Pasal 27 ayat (3), Pasal 28 ayat (2), dan Pasal 31 ayat (3) yang bertentangan dengan UUD 1945 Pasal 28 tentang kebebasan berpendapat.
8. Perlunya penjelasan secara terperinci dan lugas yang didukung oleh peraturan dibawah tingkat dari UU ITE adalah masalah *spamming*, untuk *email spamming* serta masalah penjualan data pribadi yang dilakukan oleh sektor perbankan.
9. Masih banyaknya pasal karet di dalam UU ITE ataupun pasal-pasal yang interpretasinya bersifat subjektif/individual.

Pembahasan materi dalam UU ITE terkesan tidak fokus dikarenakan banyaknya hal-hal yang diatur dalam tiap babnya. Banyak juga ketentuan pada *Convention of Cybercrime* yang tidak diatur secara khusus dalam UU ITE. Padahal *Convention of Cybercrime* adalah pedoman tentang pengaturan hukum *cybercrime* yang banyak dianut oleh negara-negara lain. Di dalam UU ITE tidak diatur secara spesifik mengenai perbuatan penipuan dengan menggunakan media komputer (*computer related fraud*) seperti yang diatur di dalam *Convention of Cybercrime*.

Perlunya perbaikan maupun perubahan dalam Undang-Undang Nomor 11 Tahun 2008 tentang *procedural law*, karena Undang-Undang Nomor 11 Tahun 2008 adalah hasil dari perpaduan antara *Convention of*

Cybercrime dan *International Telecommunication Union*. Undang-Undang Nomor 11 Tahun 2008 merupakan produk yang lengkap untuk mengatasi masalah kejahatan siber. Bahkan UU ITE diakui oleh negara lain dan dipandang cukup baik oleh akademisi negara lain tetapi kurang diapresiasi oleh negara sendiri.

3.2. Alternatif Pengaturan *Carding* Dalam *Ius Constitum* Untuk Memperbaiki Kelemahan Hukum Positif Yang Mengatur Tentang *Carding*

Perkembangan teknologi memberikan dampak yang sangat besar di berbagai bidang. Adanya perkembangan ini tentu saja memberikan banyak kemudahan yang membantu kinerja manusia dalam kesehariannya. Di era 4.0 ini, setiap orang bisa berbelanja meskipun sedang berada di rumah, bisa menghadiri rapat ataupun bekerja meskipun tidak sedang berada di kantor. Saat ini internet merupakan kebutuhan utama sekaligus menjadi faktor utama yang seakan wajib dimiliki oleh semua orang.

Seiring dengan adanya perkembangan teknologi, dampak negatif yang mengiringi perkembangan teknologi juga pasti akan timbul. *Cybercrime* merupakan salah satu contoh dampak negatif dari perkembangan teknologi yang terjadi saat ini. Menurut Gregory (2005) *cybercrime* adalah kejahatan virtual dengan menggunakan alat bantu berupa komputer yang terhubung ke jaringan internet, dan mengeksploitasi komputer lain yang terhubung dengan internet juga. Tingkat keamanan yang rendah merupakan celah pada sistem operasi mengakibatkan adanya kelemahan dan terbukanya kesempatan yang dapat

digunakan para *hacker, cracker* dan *script kiddies* untuk menerobos masuk ke dalam komputer tersebut. Dengan memanfaatkan sarana komputer dan internet, para pelaku *cybercrime* melakukan tindak kejahatannya sehingga merugikan orang lain. Aparat penegak hukum merasa kesulitan untuk menangani tindak kejahatan *cybercrime*, sulitnya untuk mengidentifikasi pelakunya apalagi jika pelaku kejahatan ini adalah *hacker* yang mahir dan profesional. Mengidentifikasinya pun juga harus menggunakan cara dan langkah yang tepat serta diidentifikasi oleh orang yang mahir pula dibidangnya.

Cybercrime menjadi sebuah masalah baru yang harus dicari solusinya. Tidak bisa pula dipungkiri bahwa dengan semakin majunya perkembangan teknologi, maka semakin maju pula perkembangan kejahatan terlebih kejahatan *cybercrime*. Positif dan negatif akan terus berjalan seiringan dan tidak bisa dipisahkan. Dan sebagai pengguna teknologi maka juga harus siap dengan dampak negatif yang muncul tersebut.

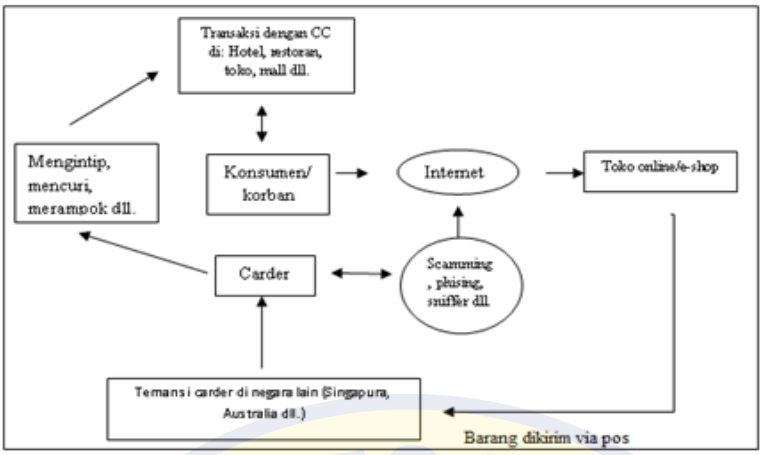
Salah satu kejahatan cybercrime adalah kejahatan *carding*. *Carding* atau yang bisa disebut juga *credit card fraud* (penipuan kartu kredit) adalah :

> *...the fraudulent acquisition and/or use of debit and credit cards, or card details, for financial gain. Card fraud may involve acquiring legitimate cards from financial institutions by using false supporting documentation (application fraud), or stealing legitimate credit and debit cards. It may also involve phishing,1 card-not-presentfraud, the creation of counterfeit cards, hacking*

> *intocompany databases to steal customer financial data, and card skimming.*
>
> Terjemahan harfiah :
>
> …perolehan penipuan dan/atau penggunaan kartu debit dan kredit, atau detail kartu, untuk keuntungan finansial. Penipuan kartu dapat melibatkan perolehan kartu yang sah dari lembaga keuangan dengan menggunakan dokumentasi pendukung palsu (penipuan aplikasi), atau mencuri kartu kredit dan debit yang sah. Ini mungkin juga melibatkan phishing, penipuan 1 kartu-tidak-hadir, pembuatan kartu palsu, meretas ke dalam basis data perusahaan untuk mencuri data keuangan pelanggan, dan skimming kartu.

Kartu kredit adalah alat transaksi elektronik, kita bisa berbelanja apa saja dengan kartu tersebut sampai dengan *limit* yang sudah ditentukan. Dalam melakukan kejahatan *carding* para *hacker* akan memanfaatkan kekurangan keamanan pada kartu kredit. Seperti tindakan kejahatan pembobolan PIN, pencurian identitas korban dan lain sebagainya. Tujuannya adalah untuk menggunakan atau membelanjakan secara illegal kartu kredit yang diperoleh ataupun untuk memperoleh dana dari pemilik yang sah. Berikut adalah gambaran modus operandi yang sering dilakukan saat ini oleh para pelaku *carding* (*carder*).

Untuk mempermudah bagaimana seorang *carder* melakukan kejahatan *carding* dapat dijelaskan menggunakan skema berikut :



Sumber: Bahan Hukum Sekunder Diolah, 2021

Berdasarkan skema tersebut dapat dipahami bahwa untuk mendapatkan identitas *user*/pemakai kartu, para *carder* menggunakan dua cara. Cara pertama yang dilakukan oleh pelaku adalah melakukan tindakan langsung untuk mendapatkannya seperti mengintip, mencuri maupun merampok para korban. Kemudian dimanfaatkan untuk melakukan transaksi di berbagai macam tempat seperti di hotel, restaurant, pusat perbelanjaan dan sebagainya.

Cara yang kedua adalah dengan cara mencuri menggunakan internet jadi tidak melakukan kontak fisik secara langsung dengan korban. Tindak kejahatan tersebut dilakukan dengan cara *scanning*, *phising* maupun melakukan *sniffer*. Setelah mendapatkan akses penuh pada kartu kredit korban, akhirnya para *carder* melakukan pembelanjaan *online* di *took online* atau *e-shop*. Barang yang dibeli kemudian dikirimkan ke teman *carder* di luar negeri, untuk nantinya dikirimkan kembali ke Indonesia.

Sebelum lahirnya UU ITE, POLRI mau tidak mau harus menggunakan pasal-pasal di dalam KUHP seperti pasal pencurian, pemalsuan dan penipuan atau penggelapan untuk menangkap para pelaku tindak kejahatan *cybercrime*, yang

dengan jelas menimbulkan kesulitan dalam hal pembuktian mengingat karakteristik tindak kejahatan *cybercrime* adalah terjadi lintas negara dan bisa dilakukan secara non fisik seperti yang sudah disebutkan seperti di atas. Dengan lahirnya UU ITE yang menangani kasus tentang transaksi elektronik, hal ini dapat dipidana dengan menggunakan pasal 31 ayat (1) ayat (2) yang membahas tentang *hacking*, padahal kejahatan *carding* dan *hacking* sangatlah berbeda modus operandinya.

Kemudian Indonesia sendiri telah memiliki undang-undang khusus untuk menangani kasus kejahatan dunia maya, yaitu Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Secara materi muatan undang-undang tersebut belum dapat menjawab persoalan kepastian hukum yang berhubungan dengan tindak pidana *carding* dan sanksi pidana yang diberikan atas tindakan atau kejahatan *carding* tersebut.

Sampai saat ini, di Indonesia belum terdapat pasal khusus yang dapat digunakan untuk menjatuhkan hukuman terhadap pelaku kejahatan *cybercrime*. Contohnya untuk kasus *carding*, kepolisian baru bisa menangkap pelaku kejahatan yang menggunakan alat bantu komputer dengan pasal 363 KUHP tentang pencurian karena yang dilakukan tersangka adalah memang mencuri data pribadi milik orang lain. Padahal modus operandi dari kejahatan *carding* ini cukup kompleks dan sangat beragam.

Hal ini dapat dibuktikan bahwa memang dalam penjelasan ketentuan umum Undang-Undang ITE yang terbaru masih belum juga memasukkan delik

pencurian data dan/atau kejahatan *carding* sebagai contoh kejahatan yang terjadi di dunia maya, sebagaimana berikut :

Melanggar kesusilaan, **perjudian**, **penghinaan** atau **pencemaran nama baik**, **pemerasan** dan/atau **pengancaman**, **penyebaran berita bohong dan menyesatkan** sehingga mengakibatkan korban mengalami kerugian dalam transaksi elektronik, serta perbuatan **menyebarkan kebencian** atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman **ancaman kekerasan** atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja merupakan karakteristik dunia maya ruang siber yang memungkinkan memiliki konten illegal.

Berdasarkan persoalan tersebut dan didukung dengan kompleksnya modus yang dilakukan oleh *carder* dalam melakukan kejahatan *carding* sebagaimana telah diuraikan pada pembahasan sebelumnya, maka perlu adanya suatu perumusan norma khusus yang mengatur tentang kejahatan *carding* dalam Undang-Undang Informasi dan Transaksi Elektronik yang akan datang dengan alternatif perumusan norma sebagai berikut :

> **Pasal (…)**
>
> Setiap orang dan/atau badan hukum dengan sengaja dan melawan hukum mengetahui dalam transaksi yang menggunakan kartu kredit adanya pemalsuan identitas, penyamaran, pengubahan, pencurian, atau penipuan, menjual atau mengangkut kartu kredit tersebut, menerima, menyembunyikan atau menggunakan kartu

kredit tersebut, dan menyediakan uang, barang, jasa, atau sesuatu yang bernilai yang diperoleh melalui kartu kredit tersebut, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan atau denda paling banyak Rp.1.000.000.000.,- (satu miliar rupiah).

Perbuatan percobaan dan pemufakatan juga termasuk dalam ketentuan tersebut untuk perbuatan-perbuatan tersebut di atas. Dengan pengaturan tersebut maka dapat dilakukan dalam tahapan alur proses kartu kredit relatif dapat terjangkau, baik dalam tahapan *source application, application processing, card embossing and delivery, usage* atau *payment to merchant,* termasuk perbuatan-perbuatan yang termasuk kejahatan kartu kredit. Demikian pula pelaku tindak kejahatan kartu kredit yang dapat dijangkau ketentuan tersebut tidak hanya pengguna kartu kredit tetapi juga pedagang, penerbit kartu kredit atau siapa pun yang mengetahui adanya pemalsuan kartu kredit, penggunaan atau peredaran kartu kredit tersebut, bahkan orang yang mencoba melakukan kejahatan kartu kredit juga diancam pidana.

Bahwa selain dari pada perlunya perumusan norma yang secara khusus mengatur kejahatan *carding,* tidak terlepas pula perlunya perlindungan hukum untuk nasabah pemegang kartu kredit sangat diperlukan seperti halnya perlindungan yang diberikan kepada nasabah penyimpan dana lainnya. Peran pemerintah sangat dibutuhkan dalam upaya menegakkan undang-undang yang mengatur tentang ITE sangatlah penting mulai dari sisi nasabah, sebab nasabah adalah orang yang paling menderita kerugian secara finansial. Menurut sistem perbankan Indonesia, terdapat dua cara untuk melindungi nasabah, yaitu :

a. Perlindungan secara eksplisit (*explicit deposit protection*) diperoleh dengan cara membentuk lembaga yang menjamin simpanan masyarakat, yang diatur di dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan Terhadap Kewajiban Bank Umum. Jadi apabila bank mengalami kebangkrutan atau kegagalan dalam pengoperasiannya, maka lembaga tersebut akan mengganti dana yang disimpan oleh masyarakat di bank yang gagal tersebut;
b. Perlindungan secara implisit (*implicit deposit protection*) yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank secara efektif. Dapat dilakukan pengawasan untuk menghindari terjadinya kegagalan bank yang diawasi.[52]

Langkah lainnya yang dapat dilakukan dalam rangka mengamankan data pribadi korban dari para *carder* adalah dengan cara sebagai berikut :

a. Melakukan penyusunan dan peninjauan kembali hukum pidana nasional beserta hukum acaranya, yang disesuaikan dengan konvensi internasional yang berhubungan dengan kejahatan tersebut. Bertujuan untuk menciptakan hukum pidana yang mengatur secara khusus kasus *cybercrime*. Serta memberikan pembelajaran bagi para pelaku kejahatan;
b. Meningkatkan kualitas sistem pengamanan jaringan komputer nasional sesuai dengan standar internasional. Aparat kepolisian yang secara

[52] Pardede, Marulak. *"Efektivitas Pengawasan Perbankan dalam Perbankan Nasional"*. Jakarta: Majalah Jurnal Hukum Bisnis, edisi September 2001. Verisign, Internet Security Intelligence Briefing, Dulles VA USA, 2004, hlm 23.

khusus menangani kasus kejahatan *cybercrime* harus melakukan peningkatan keamanan jaringan mulai dari personil, sistem informasi dan sistem keamanan. Hal pertama yang dapat dilakukan adalah membangun *firewall* untuk melindungi dari tindak kejahatan berupa penyadapan, pencurian data, *illegal access*, dan sejenisnya, serta melakukan blokade situs-situs tidak resmi dari luar negeri yang memungkinkan untuk menyebarkan *malware*, khususnya situs pornografi;

c. Mengupayakan pencegahan, investigasi dan penuntutan perkara-perkara yang berkaitan dengan *cybercrime* dengan cara meningkatkan keahlian (*skill*) dan pemahaman (*knowledge*) penegak hukum;

d. Mencegah kejahatan *carding* dengan cara meningkatkan pemahaman dan kesadaran serta ilmu pengetahuan warga negara tentang kasus *carding* serta memberi informasi pentingnya mencegah kejahatan *carding* dapat terjadi. Pencegahan dapat dimulai dari diri sendiri dengan cara memperluas pengetahuan tentang kejahatan *cybercrime* dan cara menangani/menanggulangi *cybercrime*, maka setidaknya dapat terhindar dari akibat kejahatan siber. Hal tersebut dapat dilakukan dengan cara sosialisasi pengetahuan umum tentang *cybercrime* pada masyarakat luas;

e. Menciptakan keamanan dan kewaspadaan pada diri sendiri dengan cara, jika melakukan belanja *online* dilakukan pada *online shop* yang sudah divalidasi. Menghindari menjadi anggota dalam situs yang tidak

terpercaya yang belum dibuktikan dengan pasti kebenarannya. Pencurian data sering terjadi pada anggota situs porno, *game online*, dan perjudian. Maka dari itu pentingnya kesadaran dan kewaspadaan diri dalam melakukan tindakan yang mungkin berbahaya;

f. Penanganan *cybercrime* dilakukan dengan cara peningkatkan perjanian ekstradisi dan *mutual assistance treaties*, yang merupakan bentuk kerjasama antar negara.