Jurnal Pendidikan dan Konseling
Volume 4 Nomor 6 Tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
Universitas Pahlawan Tuanku Tambusai

Analisis Kejahatan *Carding* dalam Bentuk *Cyber Crime* dan Perlindungan Hukum di Indonesia

MOHD. Yusuf DM[1], Boyke. SM[2], Rika Parlina[3]
[1]Hukum, Fakultas Hukum, Universitas Lancang Kuning
[2,3] Ilmu Hukum, Fakultas Hukum, Universitas Lancang Kuning
E-mail: boyke457@gmail.com

Abstrak

Pada saat ini perkembangan teknologi khususnya dalam bidang digital mengalami perkembangan yang sangat pesat, perkembangan teknologi juga dijadikan peluang bagi para pelaku kejahatan untuk melakukan kriminalitas di dunia maya atau media lainnya yang kerap dikenal dengan istilah *cyber crime*. Salah satu bentuk kejahatan teknologi ialah kejahatan *Carding.* Kejahatan *Carding* merupakan kejahatan mencuri data atau informasi kartu kredit orang lain secara ilegal. Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian hukum normatif yang dilakukan dengan penelitian kepustakaan. Tujuan dari penelitian ini adalah untuk memeberikan solusi bahwa dalam menangani tindak pidana *Carding,* diperlukan penegakan Undang-Undang yang kuat untuk melindungi hak-hak para korban kejahatan *Carding* agar dapat mengurangi kasus *Cyber Crime* di Indonesia.
Kata Kunci: *Carding Cyber Crime,* Undang-Undang.

Abstract

At this time technological developments, especially in the digital field, are experiencing very rapid development; technological developments are also used as opportunities for criminals to commit crimes in cyberspace or other media which is often known as Cyber Crime. One form of technology crime is Carding crime. Carding crime is the crime of illegally stealing other people's credit card data or information. The research method used in this study is a normative legal research method carried out by library research. The purpose of this study is to provide a solution that in dealing with the crime of Carding, it is necessary to enforce strong laws to protect the rights of victims of carding crimes in order to reduce Cyber Crime cases in Indonesian.
Keywords: *Carding Cyber Crime, Act.*

PENDAHULUAN

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 *Cyber Crime*. Perkembangan teknologi informasi-komputer saat ini sudah mencapai pada tahap di mana ukurannya semakin kecil, kecepatannya semakin tinggi, namun harganya semakin murah dibandingkan dengan kemampuan kerjanya. Hal ini yang menyebabkan kebutuhan akan teknologi jaringan komputer semakin meningkat.

Cyber Crime atau kejahatan melalui jaringan internet saat ini semakin tak terbendung. Di Indonesia, kejahatan ini dilakukan untuk pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer. Adanya *Cyber Crime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet. Berbagai kejahatan telah terjadi di dunia maya ini, kasus-kasus tersebut tentu saja merugikan dan berdampak negatif, kejahatan dunia maya semacam ini tidak hanya mencakup Indonesia, tetapi juga mencakup seluruh dunia.

Cyber Crime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet.[1] Kejahatan tersebut dibedakan menjadi dua kategori yakni *Cyber Crime* dalam pengertian sempit dan dalam pengertian luas. *Cyber Crime* dalam pengertian sempit merupakan kejahatan terhadap sistem komputer, sedangkan *Cyber Crime* dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.[2] Berdasarkan beberapa pendapat di atas, dapat disimpulkan bahwa *Cyber Crime* merupakan perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

Sumber-sumber ancaman Cyber dapat berasal dari berbagai sumber, seperti intelijen asing (foreign intelligence service), kekecewaan (disaffected employees), investigasi jurnalis (investigative journalist), organisasi ekstremis (extremist organization), aktivitas para hacker, dan kelompok kejahatan terorganisir (organized crime groups).[3] Semakin banyaknya kasus *Cyber Crime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *Cyber crime* (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.

Perkembangan yang pesat dalam teknologi internet berdampak munculnya berbagai macam kejahatan *cyber* atau *cyber crime*, seperti kejahatan penggunaan ilegal kartu kredit atau bisa disebut dengan kejahatan *carding*. Perkembangan dari penggunaan kartu kredit di Indonesia meningkat seiring dengan kemajuan industri perbankkan. Kartu kredit menawarkan kemudahan dalam melakukan transaksi tanpa harus menggunakan uang *cash* selain itu bentuknya yang simple dan sederhana dapat mudah dibawa kemana-mana bahkan dalam jumlah yang amat besar selain itu dipercaya lebih aman. Namun pada kenyataannya, penggunaan kartu kredit yang semakin menjamur dapat menciptakan kejahatan baru salah satunya adalah kejahatan *carding*.

Kejahatan *carding* 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* merupakan kejahatan bertransaksi memesan atau membeli barang dari dalam maupun luar negeri dengan menggunakan kartu kredit palsu untuk memperoleh suatu keuntungan.[4]

Menurut riset *Clear Commerce Inc* yang merupakan perusahaan teknologi informasi di Texas, Amerika Serikat menyatakan bahwa Indonesia memiliki pelaku kejahatan kartu kredit atau disebut dengan *carder* terbanyak kedua di dunia setelah Ukraina. Akibatnya, banyak situs belanja online memblokir IP atau *Internet Protocol* yang dari Indonesia. Menurut Wakil Kabid Informatika KADIN yang bernama Rommy Alkatiry, penyalahgunaan kartu kredit milik orang lain di internet merupakan kasus *cyber crime* terbesar yang berkaitan dengan dunia bisnis internet di Indonesia.[4]

METODE

Jenis penelitian ini adalah penelitian kepustakaan (*library research*). Penelitian kepustakaan adalah penelitian yang dilaksanakan dengan menggunakan literature (kepustakaan), baik berupa buku, catatan, maupun laporan hasil penelitian terdahulu. Penelitian ini termasuk penelitian kepustakaan karena didasarkan pada literature baik berupa buku, catatan, maupun laporan hasil penelitian terdahulu. Sehubungan dengan jenis penelitian yang digunakan yaitu penelitian hukum normatif, maka pendekatan yang digunakan adalah Pendekatan PerundangUndangan (Statute Approach), Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan yang bersangkut paut dengan permasalahan (isu hukum) yang sedang dihadapi.

Sumber data yang digunakan penelitian ini adalah data sekunder. Data sekunder adalah data yang diperoleh atau dikumpulkan oleh orang yang melakukan penelitian dari sumber-sumber yang telah ada melalui bahan-bahan kepustakaan (*library*). Teknik pengumpulan data yang digunakan adalah Studi Kepustakaan. Dalam studi kepustakaan penulis menggunakan teknik pengumpulan data dengan cara membaca, mencatat dan mempelajari bahan hukum tersebut diatas yang berkaitan dengan pengaturan *carding* dan penanggulangnya.

HASIL DAN PEMBAHASAN

Pengertian *Carding*

C*arding* 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*. Kejahatan *carding* merupakan kejahatan yang memanfaatkan teknologi internet sebagai sarana utama untuk mengakses secara tidak sah suatu sistem sebuah website untuk mendapatkan data-data para nasabah kartu kredit. Tujuannya adalah untuk membelanjakan secara tidak sah kartu kredit yang telah didapatkan ataupun untuk mendapatkan dana milik pemegang kartu kredit tersebut.[5]

Para carder memilliki dua cara untuk mendapatkan data-data kartu kredit para korban, yang pertama dengan menyentuh langsung kartu kredit milik korban yang pada umumnya dilakukan di gerai ritel seperti restoran dan toko. Tindakan tersebut dilakukan oleh karyawan dengan alasan yang sah untuk memiliki kartu kredit korban, selanjutnya karyawan memanfaatkan electronic data capture untuk mencuri data-data yang tersimpan di dalam kartu (*skimming*). Cara yang kedua adalah memanfaatkan teknologi internet.[5]

Salah satunya adalah *phising*, teknik ini digunakan oleh para carder untuk memperoleh data-data kartu kredit dengan mengarahkan korban untuk masuk ke sebuah situs website jebakan yang telah dibuat menyerupai website asli, seperti www.klikbca.com. Biasanya para carder melakukan phising dengan mengirimkan sebuah email kepada para korban. Setelah mendapatkan nomor kartu kredit beserta data-datanya, carder membelanjakannya di pedagang (merchant) online yang diinginkan. Barang yang dibeli akan dikirimkan ke alamat teman carder yang ada di luar negeri seperti Australia atau Singapura, hal ini dilakukan karena banyak merchant yang tidak berkenan mengirimkan barang ke alamat Indonesia. Setelah itu barang akan dikirimkan oleh teman carder ke alamat Indonesia.[5]

Faktor – Faktor Penyebab Terjadinya *Carding*

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 :

1) Faktor Internal

Faktor internal merupakan faktor yang ada dalam diri pelaku kejahatan *carding* bisa berupa fisik, psikis, usia, jenis kelamin, dan lain sebagainya. Berikut ini beberapa yang termasuk dalam faktor internal yang menjadi penyebab kejahatan *carding* :

a) Faktor Usia

Para pelaku dari kejahatan *carding* ini memiliki usia kurang lebih rata-rata 17 sampai 40 an tahun. Namun yang paling banyak yaitu usia 17 sampai 20 an tahun karena mereka memiliki kemampuan daya serap yang tinggi dalam menyerap suatu pengetahuan ditambah dengan sifat mereka yang cenderung memiliki keingintahuan yang tinggi pula terhadap sesuatu hal yang baru.

b) Faktor Pendidikan

Setelah faktor usia yang menjadi faktor internal penyebab kejahatan *carding* selanjutnya adalah faktor pendidikan. Faktor pendidikan merupakan faktor penting terhadap penyebab kejahatan *carding* karena pelaku kejahatan ini cenderung memiliki pendidikan yang tinggi artinya pada umumnya mereka memiliki kemampuan intelektual yang mumpuni terutama dalam bidang teknik informasi dan penguasaan komputer. Semakin tinggi kemampuan intelektual dalam bidang informasi dan penguasaan komputer seorang pelaku kejahatan *carding* maka akan semakin lihai mereka dalam melakukan aksi kejahatannya dan terkadang akan lebih sulit untuk ditangkap.

c) Faktor Percaya Diri

Pelaku kejahatan *carding* cenderung merasa percaya diri bahwa kemampuan dan pengetahuannya sudah cukup untuk melakukan kejahatan ini. Mereka mempunyai tingkat kepercayaan yang tinggi untuk segera mencoba melakukan kejahatan ini dengan tujuan mendapatkan kentungan tanpa takut tertangkap oleh polisi.

d) Faktor Peluang

Faktor peluang maksudnya bahwa pelaku kejahatan *carding* memanfaat peluang sebaik mungkin agar dapat memperoleh data-data yang diingankan. Dengan berbekal pengetahuan yang telah dipelajari, mereka dapat melakukan kejahatan *carding* dengan berbagai cara dan kemungkinan sehingga dapat memperhitungkan peluang yang diperoleh dengan baik.

2) Faktor Eksternal

Faktor eksternal merupakan faktor yang berada di luar dari pelaku kejahatan *carding* biasanya terletak pada lingkungannya. Berikut ini beberapa faktor yang termasuk ke dalam faktor eksternal penyebab kejahatan *carding* adalah sebagai berikut :

a) Faktor Perkembangan Teknologi

Perkembangan teknologi khususnya teknologi informasi dan komunikasi selain memberikan dampak positif juga memberikan dampak negatif terhadap masyarakat diseluruh dunia karena selain dapat mengubah perilaku dan peradapan manusia serta menyebabkan perubahan soaial, perkembangan teknologi informasi yang meningkat membuat dunia menjadi tanpa batas sehingga banyak muncul kejahatan baru yang memanfaat internet sebagai modus operandinya salah satunya adalah kejahatan *carding*.

b) Faktor Ekonomi

Faktor ekonomi mrupakan faktor yang paling banyak dijadikan alasan untuk mendorong seseorang melakukan kejahatan. Dalam kasus kejahatan *carding* biasanya pelaku memiliki

hasrat untuk membeli sesuatu barang yang diinginkan atau untuk memenuhi kebutuhan sehari-harinya tanpa harus mengeluarkan uang dari sakunya karena uang yang dia miliki tidak mencukupi. Mereka mengambil jalan pintas dengan melakukan kejahatan *carding* tanpa harus mengeluarkan banyak tenaga. Keadaan ekonomi yang tidak menguntungkan memberikan jarak antara harapan, keinginan dan kemampuan untuk mencapainya.

c) Faktor Kesadaran Hukum Masyarakat

Kesadaran hukum masyarakat Indonesia terhadap kejahatan di dunia maya khususnya kejahatan *carding* masih sangat lemah. Hal ini disebabkan oleh kurangnya pengetahuan masyarakat tentang apa dan bagaimana jenis-jenis kejahatan di dunia maya. Pengetahuan dan pemahaman terhadap kejahatan ini sangat dibutuhkan supaya masyarakat lebih waspada atau lebih peka terhadap kejahatan di dunia maya khususnya kejahatan *carding*.[4]

Sistem Hukum yang berlaku di Indonesia mengenai Kejahatan *Carding*

Cyber crime sudah diatur dalam hukum spesial ialah UndangUndang No 11 Tahun 2008 mengenai Data serta Transaksi Elektronik dimana cocok dengan dasar hukum lex specialis derogate legi generali bisa jadi referensi buat memerangkap pelakon kesalahan *carding* atau kesalahan yang lain yang berhubungan dengan penyalahgunaan teknologi data. Tetapi pada faktanya dalam menanggulangi masalah kejahatan yang melanggar ketetapan kejahatan biasa ataupun eksklusif sekalian tidak sedikit yang sedang memakai ketetapan hukum biasa sementara itu dalam perlengkapan fakta yang terdapat telah nyata dikenal kalau aksi pelakon sudah penuhi determinasi hukum spesial.

Terdapat sebagian hukum positif yang legal biasa serta bisa dikenakan untuk para pelaksana *cyber crime* paling utama buat kasuskasus yang memakai komputer selaku prasarana, antara lain:

1) Kitab Undang Undang Hukum Pidana Dalam usaha menanggulangi kasus- kasus yang terjalin para pemeriksa melaksanakan kemiripan ataupun ibarat serta persamaaan kepada Pasal- Pasal yang terdapat dalam KUHP. Pasal-Pasal didalam KUHP umumnya dipakai lebih dari satu Artikel sebab mengaitkan sebagian aksi sekalian Pasal- Pasal yang bisa dikenakan dalam KUHP pada *cyber crime* antara lain :
   a) Pasal 362 KUHP yang dikenakan buat permasalahan *carding* dimana pelakon mencuri no kartu angsuran kepunyaan orang lain meski tidak dengan cara raga sebab nomor kartunya saja yang didapat dengan memakai aplikasi card generator di Internet buat melaksanakan bisnis di ecommerce. Sehabis dicoba bisnis serta benda dikirimkan, setelah itu pedagang yang mau melarutkan uangnya di bank nyatanya ditolak sebab owner kartu tidaklah orang yang melaksanakan bisnis.
   b) Pasal 378 KUHP bisa dikenakan buat pembohongan dengan seakan olah menawarkan serta menjual sesuatu produk ataupun benda dengan memasang promosi di salah satu web alhasil orang terpikat buat membelinya kemudian mengirimkan duit pada pemasang promosi. Namun, pada faktanya, benda itu tidak terdapat. Perihal itu dikenal sehabis duit dikirimkan serta benda yang dipesankan tidak tiba alhasil konsumen itu jadi terkecoh.
   c) Pasal 335 KUHP bisa dikenakan buat permasalahan penggertakan serta eksploitasi yang dicoba lewat e-mail yang dikirimkan oleh pelakon buat memforsir korban melaksanakan suatu cocok dengan apa yang di idamkan oleh pelakon serta bila tidak dilaksanakan hendak bawa akibat yang mematikan. Perihal ini umumnya dicoba sebab pelakon umumnya mengenali rahasia korban.
   d) Pasal 311 KUHP bisa dikenakan buat permasalahan kontaminasi julukan bagus dengan memakai alat Internet. Modusnya merupakan pelakon mengedarkan e-mail pada sahabat korban

mengenai sesuatu narasi yang tidak betul ataupun mengirimkan e-mail ke sesuatu mailing list alhasil banyak orang mengenali narasi itu.

e) Artikel 303 KUHP bisa dikenakan buat memerangkap game gambling yang dicoba dengan cara online di Internet dengan eksekutor dari Indonesia.
f) Pasal 282 KUHP bisa dikenakan buat penyebaran pornografi ataupun web porno yang banyak tersebar serta gampang diakses di Internet. Meski berbicara Indonesia, amat susah sekali buat menangani pelakunya sebab mereka melaksanakan registrasi daerah itu diluar negara dimana pornografi yang menunjukkan orang berusia bukan ialah perihal yang bawah tangan.
g) Pasal 282 serta 311 KUHP bisa dikenakan buat permasalahan penyebaran gambar ataupun film individu seorang yang cabul di internet, misalnya permasalahan Sukma Ayu- Bjah.
h) Pasal serta 262 KUHP bisa dikenakan pada permasalahan *carding*, sebab pelakon melaksanakan pembohongan seakan mau membeli sesuatu benda serta melunasi dengan kartu kreditnya yang no kartu kreditnya ialah jarahan.
i) Pasal 406 KUHP bisa dikenakan pada permasalahan deface ataupun hacking yang membuat sistem kepunyaan orang lain, semacam web ataupun program jadi tidak berperan ataupun bisa dipakai begitu juga mestinya.

2) Undang-Undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik. UU ITE dipersepsikan selaku cyberlaw di Indonesia, yang diharapkan dapat menata seluruh hal bumi Internet (siber), tercantum didalamnya berikan punishment kepada pelaksana *Cyber Crime*. *Cyber Crime* dideteksi dari 2 ujung penglihatan:
   a) Kesalahan yang Memakai Teknologi Data Selaku Sarana: Pemalsuan, Pornografi, Manipulasi atau Perampokan Kartu Angsuran, Pembohongan Melalui Email (Fraud), Email Spam, Pertaruhan Online, Perampokan Account Internet, Terorisme, Rumor Sara, Web Yang Menyesatkan, dsb.
   b) Kesalahan yang Menghasilkan Sistem Teknologi Data Selaku Target: Perampokan Informasi Individu, Pembuatan atau Penyebaran Virus Pc, Pembobolan atau Pembajakan Situs, C*yberwar*, *Denial of Service (DOS)*, Kesalahan Berkaitan Dengan Julukan Daerah, dsb.

Cyber Crime jadi rumor yang menarik serta kadangkala mengalutkan sebab:

a) Aktivitas dunia cyber tidak dibatasi oleh kedaerahan negeri.
b) Aktivitas dunia cyber relatif tidak berbentuk.
c) Sulitnya pembuktian sebab informasi elektronik relatif gampang buat diganti, disadap, dipalsukan serta dikirimkan ke semua bagian bumi dalam hitungan detik.
d) Pelanggaran hak membuat dimungkinkan dengan cara teknologi.
e) Telah tidak membolehkan lagi memakai hukum konvensional.[6]

SIMPULAN

Berdasarkan pembahasan di atas dapat disimpulkan bahwa *Carding* adalah kejahatan dengan menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan kartu kredit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non-materil. *Carding* merupakan tindak pidana karena unsur-unsur perbuatan dalam proses kejahatan *carding* telah diatur dalam peraturan perundang-undangan, maka dapat dikatakan untuk kejahatan ini dapat digunakan pasal-pasal dari hukum pidana positif Indonesia, yakni Pasal 263, 362, 378 KUHP dan Pasal 30 UU ITE. Oleh karena itu, dalam penanggulangannya dibutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut, selain itu juga diperlukan adanya kerja sama dengan lembaga khusus untuk memberikan informasi tentang *Cyber Crime*, melakukan sosialisasi

secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan *Cyber Crime*.

DAFTAR PUSTAKA

D. Z. Abidin, "Kejahatan dalam Teknologi Informasi dan Komunikasi," *J. Ilm. Media Process.*, vol. 10, no. 2, pp. 1–8, 2015, [Online]. Available: http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107/105

H. S. Sumarwani, "Tinjauan Yuridis Pemidanaan *Cyber Crime* Dalam Perpektif Hukum Pidana Positif," *J. Pembaharuan Huk.*, vol. 1, no. 3, pp. 287–296, 2014, [Online]. Available: http://jurnal.unissula.ac.id/index.php/PH/article/view/1489

I. Rahmawati, "the Analysis Of Cyber Crime Threat Risk Management To Increase Cyber Defense," *J. Pertahanan Bela Negara*, vol. 7, no. 2, pp. 51–66, 2017, doi: 10.33172/jpbh.v7i2.193.

S. C. Widayati, A. Normasari, and I. H. Laili, "Penggunaan Ilegal Kartu Kredit (Carding) Ditinjau Dari Uu Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Din. Huk. dan Masy.*, vol. 1, no. 2, p. 3, 2020.

[N. A. Kurniawan, "Pencegahan Kejahatan Carding Sebagai Kejahatan Transnasional Menurut Hukum Internasional," *Kumpul. J. Mhs. …*, 2014, [Online]. Available: http://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/632

H. S. Arnold Bagas Kurniawan, "Perlindungan Hukum Kepada Pengguna Elektronik Banking Atas Kejahatan Carding Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik," vol. 5, no. 01, pp. 65–87, 1945.