

PERTANGGUNGJAWABAN HUKUM PENGAKSESAN KARTU KREDIT TANPA HAK DENGAN SISTEM PERETASAN MELALUI WEBSITE DITINJAU DARI PASAL 32 AYAT (1) UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

*Legal Responsibility Of Accessing Credit Cards Without Rights Using A Hacking System Through The Website Is
Reviewed From Article 32 Paragraph (1) Of Law Number 19 Of 2016 Concerning Amendments To
Law Number 11 Of 2008 Concerning Electronic Information And Transactions*

Farid Satriya Pratama¹ Sylvia Setjoatmadja²
Fakultas Hukum Universitas Gresik Jl Arif Rahman
Hakim No. 2B Gresik

Email : Faridsatria88@gmail.com¹ sylviasetjoatmadja@unigres.ac.id²

Abstrak

Peretasan yang dilakukan dengan menjebol, melampaui atau menerobos sistem elektronik yang digunakan oleh pemerintah atau untuk informasi publik merupakan tindak pidana yang dilakukan untuk ketenaran maupun keisengan hacker., rumusan masalah penelitian ini adalah : Bagaimana sistem peretasan kartu kredit tanpa hak melalui *website* dan Bagaimana pertanggungjawaban hukum terhadap tindak pidana pengaksesan kartu kredit tanpa hak dengan sistem peretasan melalui *website*.

Jenis penelitian ini adalah penelitian normatif, dimana pendekatan terhadap permasalahan dengan mengkaji ketentuan perundangan-undangan, konseptual dan kasus. Kesimpulan yang didapat yaitu *Hacking* dirumuskan Pasal 32 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Dan menurut Pasal 48 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik menyebutkan : “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.000,- (dua miliar rupiah)”.

Saran penulis adalah Mengingat dampak yang ditimbulkan tindak pidana *hacking* sangat berbahaya bagi *privasi* seseorang maupun instansi atau lembaga hukum maka hendaknya pemilik situs atau *website* memberikan pengamanan *software* komputer baik berupa penggunaan *firewall*.

Kata Kunci: Pertanggung jawaban, Penyelenggara Jalan, Kecelakaan

PENDAHULUAN

Latar Belakang

Di era globalisasi komunikasi yang semakin terpadu dan terdepan dengan internet yang menjadi sangat populer dikalangan masyarakat sekarang seakan telah membuat dunia menciut dan memudahkan batas negara berikut peraturan dan tatanan masyarakatnya. Pemanfaatan internet yang

semakin meluas dalam berbagai aktivitas kehidupan manusia, bukan saja di negara-negara maju tapi juga di negara-negara berkembang termasuk Indonesia. Fenomena ini pada gilirannya telah menempatkan informasi sebagai komoditas ekonomi yang sangat

penting dan menguntungkan.¹ Dalam Pasal 1 angka 2 (dua) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik menyebutkan transaksi elektronik yaitu : “Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya”.

Perkembangan zaman saat ini sangatlah besar, terutama dengan adanya perkembangan kemajuan teknologi yang membawa perubahan besar terhadap pola hidup manusia. Teknologi ini sangat membantu manusia dalam melakukan berbagai kegiatan, misalnya dalam berinteraksi dengan sesama, berkomunikasi, juga untuk mencari berita lewat media elektronik, bahkan bisa juga untuk melakukan bisnis perdagangan yang tanpa harus pergi kemanapun, jual beli online saat ini sedang eksis, karena banyak orang yang melakukan transaksi melalui online.

Secara khusus negara hukum merupakan negara yang menjadikan hukum sebagai kekuasaan tertinggi. Konsekuensi ketentuan ini adalah bahwa setiap sikap, kebijakan, dan perilaku aparat negara dan penduduk harus sesuai aturan hukum yang berlaku.² Bahkan ketentuan ini untuk mencegah terjadi kesewenang-wenangan dan arogansi kekuasaan, baik yang dilakukan aparat negara maupun penduduk. Dalam kehidupan sehari-hari hukum merupakan salah satu bidang yang sangat erat kaitannya dengan perilaku seseorang, tidak dapat dipungkiri bahwa hampir sebagian besar aspek kehidupan manusia mulai sejak didalam kandungan sampai sejak ia dilahirkan sebagai makhluk sosial itu semua diatur di dalam hukum.

Memenuhi kebutuhan hidup merupakan wajib bagi setiap orang demi keberlangsungan hidupnya, hal ini pun tidak terlepas dari aturan hukum yang ada. Namun seiring dengan berkembangnya ekonomi global yang memberi dampak pada Negara Indonesia berupa fenomena yaitu tidak bisa lagi semudah membalik telapak tangan dalam memenuhi kebutuhan seseorang. Seseorang dalam memenuhi kebutuhan saat ini cenderung menghalalkan segala cara baik maupun buruk. Apalagi kebutuhan tersebut merupakan sesuatu yang harus segera dipenuhi terkadang tidak lagi mempertimbangkan cara untuk memenuhinya. Selain itu, mayoritas masyarakat telah

menginginkan segala sesuatu yang dimiliki haruslah yang praktis dan ekonomis terutama dalam hal sistem pembayaran atau transaksi.³

Ketentuan mengenai peretasan dan penyadapan informasi tertuang dalam Pasal 32 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik menyebutkan transaksi elektronik menyebutkan :

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik;

Di era modern saat ini sistem pembayaran lebih mudah karena tersedia dalam bentuk elektronik dan tanpa uang tunai seperti melalui *M-banking* maupun kartu kredit. Kartu kredit merupakan salah satu alat teknologi akibat munculnya kemajuan internet. Kartu kredit kerap kali dijadikan sebagai bahan kejahatan melalui teknologi internet, karena praktek industri kartu kredit di Indonesia masih dalam kategori belum aman. Segala aktivitas kehidupan masyarakat modern saat ini telah berkaitan erat dengan segi ekonomi yaitu melalui transaksi.

Transaksi tersebut bisa melalui *e-banking* dan *e-commerce* sebab sangat mudah digunakan dalam bertransaksi secara online. *E-banking* adalah sistem aplikasi yang membuat penggunaanya mampu melakukan segala hal yang berkaitan dengan bank secara online hanya dengan menggunakan *smartphone*. Sedangkan *e-commerce* adalah layanan pemenuhan kebutuhan secara online melalui website atau internet, dimana dalam setiap transaksinya memerlukan kartu kredit untuk pembayaran.⁴

Secara singkat kejahatan dunia maya (*cybercrime*) dapat diartikan dengan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. *Cyber crime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat, luas bagi seluruh bidang kehidupan modern saat ini.⁵ Percepatan industri perbankan menyebabkan meningkatnya pemakai kartu kredit, karena alat ini

¹ Abdul Halim Barakatullah, Teguh Prasetyo, “*Bisnis E-Commerce Studi System Keamanan dan Hukum di Indonesia*”, Pustaka Pelajar, Yogyakarta, 2006, h. 1.

² Putera Astomo, “*Prinsip-Prinsip Negara Hukum Indonesia Dalam UUD NRI Tahun 1945*”, Jurnal Hukum, Ilmu Hukum FISIP UNSULBAR, Vol. 1, Nomor 1 Januari, Universitas Sulawesi Barat, 2017, h. 2.

³ Zainal Arief M, “*Tinjauan Yuridis Penyalahgunaan Kartu Debit Sebagai Tindak Pidana Informasi Dan*

Transaksi Elektronik (Studi Kasus Putusan Nomor. 1985/Pid.B/2012/PN.MKS)”, Skripsi, Sarjana Hukum, Fakultas Hukum Universitas Hasanuddin, Makassar, 2016, h. 2.

⁴ *Ibid.*

⁵ Barda Nawawi Arief, “*Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*”, PT Raja Grafindo Persada, Jakarta, 2007, h. 1.

dapat memberikan kemudahan dalam melakukan transaksi mulai dari bentuk yang praktis dan komoditas dari kartu ini adalah kita bisa membayar tanpa menggunakan uang tunai. Dampak dari kemudahan ini menimbulkan motif kejahatan baru yang disebut *carding*.⁶ *Carding* merupakan Salah satu kejahatan dengan motif menggunakan kartu kredit.

Motif kejahatan ini adalah berbelanja dengan menggunakan identitas dan nomor orang lain, dengan metode mencuri data pribadi seseorang melalui internet, bukan hanya transaksi dalam pembelian tiket pesawat maupun hotel serta barang barang lainnya tetapi saat ini seiring dengan perkembangan dan munculnya banyak aplikasi yang memudahkan transaksi membuat hacking lebih mudah mentransfer uang orang luar negeri masuk ke rekening mereka dengan menggunakan aplikasi Cash App yang kemudian ditampung dalam sebuah aplikasi Cash App setelah berhasil kemudian *cash out* dan transfer masuk ke rekening milik pelaku tindak pidana *hacker*.

Modus pencurian data pribadi dari sejumlah sistem elektronik tersebut diatas terjadi karena adanya akses ilegal pelaku dengan menggunakan *malware* pencuri data. Cara kerja *malware* pencuri data tersebut yaitu melalui *Exploit Kit* dan *spam* email yang berkedok *invoice* palsu. Ketika pengguna membuka atau mengunduh kiriman tersebut secara tidak sadar pengguna mengeksekusi *malware* tersebut. Kemudian setelah itu komputer yang terinfeksi akan terhubung dengan server penyerang (*C2 server*) untuk menerima dan mengirim pesan, sehingga pelaku dapat mengakses data pribadi pengguna yang seharusnya tersimpan secara aman.⁷

Peretasan yang dilakukan dengan menjebol, melampaui atau menerobos sistem elektronik yang digunakan oleh pemerintah atau untuk informasi publik merupakan tindak pidana yang dilakukan untuk ketenaran maupun keisengan *hacker*. Kejahatan dunia maya (*Cybercrime*) adalah tindak pidana yang dilakukan pada teknologi internet (*cyberspace*). Peretasan merupakan bagian dari *cybercrime*. Peretas adalah orang yang mempelajari, menganalisis, memodifikasi, dan menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan.⁸

Sedangkan kerugian berupa moril dapat berupa tercemarnya nama baik seseorang bukan hanya orang tetapi negarapun akan tercoreng nama baiknya oleh negara asing akibat dari peretasan informasi data

pribadi (kartu kredit) milik orang lain dalam website tanpa izin dari pemiliknya.⁹

Bahwa tindak pidana *cyber* tidak lagi dilakukan di 1 (satu) Negara akan tetapi sudah merambah tindak pidana antar Negara Seperti contoh kasus perkara nomor : 500/Pid.Sus/2019/PN Jkt.Sel, di Jakarta Selatan yaitu Awal mulanya sdr. Abdul Harist alias Haris Bin Oyo Sunaryo (berkas dilakukan terpisah) membuat promo-promo untuk dimasukkan ke Akun Instagram Prime Ticket dan juga ke *Carousell* singapore dengan website “*www.carousell.com*” dengan nama akun miliknya “*primeticketsg*” untuk mendapatkan customer di singapore. Dalam website tersebut Sdr. Abdul Harist berkenalan dengan Sdri.

Janice Guyab warga Filipina (belum tertangkap) bertempat tinggal di Singapore dan sekitar bulan Desember 2017, Sdri. Janice Guyab membeli tiket penerbangan *Cathay Pasific Air* untuk dirinya sendiri.

Selanjutnya Sdr. Abdul Harist kerja sama dengan Sdri. Janice Guyab memberikan promo-promo melalui akun instagram. Kemudian dalam menjalankan aksinya, Sdri. Janice Guyab menerima pembayaran dari customer selaku pemesan tiket dan memberikan detail penerbangan dan penumpang kepada Terdakwa I Abimanyu dan juga membayar atau mentransfer kepada Terdakwa I Abimanyu melalui rekening di Bank Central Asia (BCA), atas nama Terdakwa III Rizqy Malino (adiknya Terdakwa I Abimanyu) sebesar 50% (lima puluh persen).

Akibat perbuatan yang dilakukan Terdakwa I Abimanyu Hamidigo, Terdakwa II Ahmad Hafiz Alqodri Lubis dan Terdakwa III Rizqy Malino bersama Sdr. Abdul Harist, sehingga berhasil mengakses tiket penerbangan *singapore airline* secara tidak resmi dari agen tiket “Prime Ticket” untuk berbagai tujuan penerbangan, yang mana agen tiket “Prime Tiket” melakukan pembelian tiket tersebut secara online dengan mengirimkan email palsu/fiktif (*spam*) dari pengguna kartu kredit Bank DBS dan mengambil data dari pengguna kartu kredit Bank DBS hingga mendapat data kartu kredit dengan menggunakan situs resmi *www.singaporeair.com* dari bulan Maret 2018 s.d. Mei 2018 dengan nilai kerugian sebesar Rp.101.400.000,- (seratus satu juta empat ratus ribu rupiah) karena faktanya Sdr. Wong Yik Teru pemilik asli kartu kredit Bank DBS dan Sdr. Field James Michael pemilik asli kartu kredit Bank DBS tidak pernah melakukan transaksi pembelian dan atau pemesanan tiket *singapore airline*.

⁶ Mehda Zuraida. “*Credit Card Fraud (Carding) dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia*”, Jurnal Analisis Hubungan Internasional, Vol. 4. No. 1. Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Airlangga, Surabaya, 2015, h. 1629.

⁷ Kristian dan Yopi Gunawan, “*Sekelumit tentang Penyadapan dalam Hukum Positif di Indonesia*”, Nuansa Aulia, Bandung, 2013, h. 4.

⁸ Ancaman Hacker Website, “*Hacker Selalu Menjadi Ancaman Serius Bagi Keamanan Berbagai Kegiatan*”, <https://thidiweb.com/ancaman-hacker-website/>, Online diakses pada 13 Desember 2023, pukul 19.23.

⁹ *Ibid*.

Oleh karena itu penulis tertarik untuk mengangkat suatu judul penelitian “Pertanggungjawaban Hukum Terhadap Tindak Pidana Pengaksesan Kartu Kredit Tanpa Hak Dengan Sistem Peretasan Melalui Website Ditinjau Dari Pasal 32 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik”.

Rumusan Masalah

1. Apakah pengaksesan informasi tanpa hak melalui *website* termasuk perbuatan melawan hukum?
2. Bagaimana bentuk pertanggungjawaban hukum pelaku tindak pidana pengaksesan kartu kredit tanpa hak dengan sistem peretasan melalui *website*?

Tujuan

1. Untuk mengetahui pengaksesan informasi tanpa hak melalui *website* termasuk perbuatan melawan hukum.
2. Untuk mengetahui bentuk pertanggungjawaban hukum pelaku tindak pidana pengaksesan kartu kredit tanpa hak dengan sistem peretasan melalui *website*.

Metode Penelitian

Metode penelitian ini merupakan cara yang digunakan untuk mendapatkan data serta memperoleh jawaban yang akurat atas rumusan masalah diatas dengan mencari dan mengelola data dalam suatu penelitian. Metode penelitian ini terdiri dari:

1. Jenis Penelitian: Jenis penelitian ini adalah penelitian hukum normatif, penelitian hukum untuk menemukan aturan hukum, prinsip-prinsip hukum maupun doktrin-doktrin hukum. Peneliti akan mendapatkan informasi dari berbagai aspek mengenai isu yang sedang dicoba untuk dicari jawaban. Hasil dari penelitian ini memberikan preskripsi mengenai rumusan masalah yang diajukan, penelitian normatif hanya meneliti norma hukum, tanpa melihat praktek hukum di lapangan (*law in action*). Terkait pertanggungjawaban hukum pelaku tindak pidana pengaksesan kartu kredit tanpa hak dengan sistem peretasan melalui *website*.
2. Pendekatan: Metode pendekatan merupakan salah satu tahapan penelitian yang dimaksudkan untuk mengumpulkan bahan-bahan dalam berbagai aspek untuk mencari jawaban atas permasalahan yang telah dirumuskan dalam penelitian ini. Adapaun dalam penelitian ini penulis menggunakan 3 (tiga) metode pendekatan antara lain pendekatan konseptual

(*conceptual approach*), pendekatan perundang-undangan (*statute approach*), dan pendekatan kasus (*case approach*).

3. Metode Pengumpulan Bahan: Dalam penelitian hukum normatif, teknik pengumpulan bahan hukum dengan cara bahan hukum primer berupa perundang-undangan dikumpulkan dengan metode inventarisasi dan kategorisasi. Sedangkan bahan hukum sekunder dikumpulkan dengan sistem kartu catatan (*card system*), baik dengan kartu ikhtiar (memuat ringkasan tulisan sesuai aslinya, secara garis besar dan pokok gagasan yang memuat pendapat asli penulis), maupun kartu ulasan (berupa analisis dan catatan khusus penulis).
4. Teknik Analisa Bahan: Analisis bahan hukum dalam penelitian ini berdasarkan bahan yang ada dilakukan secara yuridis kualitatif, yaitu tidak hanya mengungkapkan kebenaran belaka tetapi juga memahami kebenaran tersebut menurut aturan perundang-undangan. Dengan memberikan gambaran permasalahan tentang pertanggungjawaban hukum pelaku tindak pidana pengaksesan kartu kredit tanpa hak dengan sistem peretasan melalui *website*.

PEMBAHASAN

PENGAKSESAN INFORMASI TANPA HAK MELALUI WEBSITE TERMASUK PERBUATAN MELAWAN HUKUM

Kejahatan Dunia Maya (Cybercrime)

Sebelum mengurai pengertian kejahatan dunia maya (*cybercrime*) secara terperinci, maka terlebih dahulu akan dijelaskan “induk” kejahatan dunia maya (*cybercrime*) yaitu *cyber space*. *Cyber space* dipandang sebagai sebuah dunia komunikasi berbasis komputer. Dalam hal ini, *cyber space* di anggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan internet.¹⁰

Realitas baru ini dalam kenyataannya terbentuk melalui jaringan komputer yang menghubungkan antar negara atau antar benua yang berbasis protokol. Hal ini berarti, dalam sistem kerjanya dapatlah dikatakan bahwa internet (*cyberspace*) telah mengubah jarak dan waktu menjadi tidak terbatas. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda.¹¹ Dalam perkembangan selanjutnya kehadiran teknologi canggih komputer dengan jaringan internet telah membawa manfaat besar bagi

¹⁰ Maskun, “Kejahatan Siber Cyber Crime”, Kencana, Jakarta, 2013, h. 46.

¹¹ Ibid.

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. Kejahatan Dunia Maya (*cybercrime*) merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional (*street crime*).¹²

Cybercrime muncul bersamaan dengan lahirnya revolusi teknologi informasi. Pada masa awalnya, *cybercrime* didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para ahli belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan penggunaan istilah tindak pidana untuk kejahatan komputer dalam bahasa Inggris pun masih belum seragam. Beberapa ahli menggunakan istilah *computer misuse*, *computer abuse*, *computer fraud*, *computer related crime*, *computer assistend crime*, atau *computer crime*.¹³ Namun para ahli pada waktu itu, pada umumnya lebih menerima pemakaian istilah *computer crime* oleh karena dianggap lebih luas dan bias dipergunakan dalam hubungan internasional.

Akan tetapi, kemajuan teknologi informasi (internet) dan segala bentuk manfaat di dalamnya membawa konsekuensi negatif tersendiri di mana semakin mudahnya para penjahat untuk melakukan aksinya yang semakin meresahkan masyarakat.¹⁴ Penyalahgunaan yang terjadi dalam internet (*cyber space*) atau dalam kata lain Kejahatan Dunia Maya (*cybercrime*). Secara etimologi *cybercrime* berasal dari dua rangkaian kata, yaitu *cyber* dan *crime*. Menurut Kamus Bahasa Inggris-Indonesia *cyber* berarti maya, sedangkan *crime* diartikan dengan kejahatan.¹⁵

Menurut *Dictionary of Contemporary English*, *crime* adalah *an offence which is punishable by law* (suatu kejahatan yang dihukum oleh hukum), *illegal activity in general* (kegiatan ilegal pada umumnya), atau *a bad, immoral, or dishonourable act* (tidak terhormat, tidak bermoral, atau tindakan yang buruk).¹⁶ Secara kebahasaan *cybercrime* semakna

dengan “kejahatan dunia maya” atau “kejahatan mayantara”.

Secara umum kejahatan yang berbasis pada teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu *computer misuse*, *computer abuse*, *computer fraud*, *computer-related crime*, *computer-assisted crime*, atau *computer crime*. Muladi dalam bukunya yang ditulis bersama Barda Nawawi Arief memandang *cybercrime* dengan pendekatan *computer crime* (kejahatan komputer). Namun demikian, *cybercrime* sesungguhnya berbeda dengan *computer crime*.¹⁷ *Cybercrime* di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer, akan tetapi melibatkan teknologi telekomunikasi di dalam pengoperasiannya.

Hal ini juga dikemukakan oleh Agus Raharjo, bahwa istilah *cybercrime* sampai saat ini belum ada kesepakatan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cyber crime* dengan *computer crime*.¹⁸ Barda Nawawi Arief menggunakan istilah “tindak pidana mayantara” untuk menyebut *cybercrime*. Barda Nawawi Arief mengatakan, dengan istilah “tindak pidana mayantara” dimaksudkan identik dengan tindak pidana di ruang cyber (*cyber space*) atau yang biasa juga dikenal dengan istilah “*cybercrime*”.¹⁹

Indra Safitri yang mengemukakan pandangannya bahwa *cybercrime* adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah sistem teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.²⁰

Dari berbagai pengertian *computer crime* di atas, dapat dikemukakan rumusan definisi *cybercrime* yang tidak jauh substansinya dari pengertian yang disebutkan oleh para ahli tersebut. Hal ini dimaksudkan sebagai bentuk ketegasan dalam menarik benang merah dari perbedaan yang ada, sehingga pengertian *cyber crime* dapat tergambar secara jelas dan mudah dipahami. Adapun menurut Widodo bahwa *cybercrime* adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sarana

¹² *Ibid*, h. 47.

¹³ Widyopramono Hadi Widjojo, “Cybercrimes dan Pencegahannya”, jurnal Hukum Teknologi, Fakultas Hukum Universitas Indonesia, Jakarta, 2005, h. 7.

¹⁴ *Ibid*.

¹⁵ John M. Echols dan Hassan Shadily, “Kamus Inggris-Indonesia Cet. XXV”; Gramedia Pustaka Utama, Jakarta, 2003, h. 155.

¹⁶ *Ibid*.

¹⁷ Agus Rahardjo, “Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi”, Citra Aditya Bakti, Bandung, 2002, h. 227.

¹⁸ *Ibid*.

¹⁹ Barda Nawawi Arief, “Kapita Selekta Hukum Pidana”, Citra Aditya Bakti, Bandung, 2003, h. 239.

²⁰ Maskun, *Op.Cit*, h. 47.

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.²¹

Maka *cybercrime* merupakan setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan yang bertentangan dengan peraturan perundang-undangan, baik melawan hukum secara materiil maupun melawan hukum secara formil.²² *Cybercrime* dapat dimaknai secara luas dan sempit, *cybercrime* dapat dimaknai sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer, sedangkan dalam arti luas, *cybercrime* merupakan keseluruhan bentuk kejahatan konvensional yang menggunakan teknologi komputer.²³

Sehingga tindak pidana *cybercrime* merupakan suatu tindak pidana yang dilakukan dengan menggunakan jaringan teknologi informasi komputer untuk mendapatkan data secara ilegal serta dipergunakan untuk mengambil keuntungan yang tidak sah dan menyebabkan kerugian pada masyarakat. Kejahatan dunia maya (*cyber crime*) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Terutama pada era globalisasi saat ini yang membawa kemajuan teknologi yang sangat pesat, maka hal tersebut tidak terlepas dari resiko dari penyalahgunaan pemanfaatan teknologi sebagai kebutuhan informasi.²⁴ Maka, dapat disimpulkan bahwa *cybercrime* merupakan suatu kejahatan baru yang berhubungan dengan teknologi informasi atau dunia maya (*cyber space*), yang mana kejahatannya dilakukan melalui sistem elektronik dengan jaringan internet yang berbasis komputer dan komputer dijadikan sebagai sarana atau alat untuk melakukan kejahatan.

Jenis-Jenis Kejahatan *Cybercrime*

Seperti halnya definisi dari *cybercrime*, jenis-jenis *cybercrime* juga berbeda-beda, karena setiap ahli memiliki pendapat yang berbeda-beda, selain itu juga belum ada kesepakatan yang seragam mengenai pengertian *cybercrime* membuat banyaknya perbedaan tersebut. Nazura Abdul Manap berpendapat, kejahatan *cybercrime* dapat dibedakan ke dalam 3 (tiga) kelompok kategori, yaitu:²⁵

1. pertama, *cybercrimes against property* (kejahatan maya terhadap hak milik).

Misalnya, pencurian informasi properti, dan pelayanan, *fraud* atau *cheating*, *forgery*, dan *mischief*. Tiga yang terakhir menyangkut perilaku penipuan, pemaksaan, penjangbretan, dan yang sejenis;

2. Kedua, *cyber crimes against Persons* (kejahatan maya terhadap orang). Kejahatan ini meliputi pornografi, *cyber harassment* (pelecehan, seperti pelecehan seksual, terhadap seseorang melalui dunia maya), *cyber stalking* (mengejar-ngejar seseorang atau mengikuti terus-menerus sehingga mengganggu orang yang dikejar-kejar), dan *cyber trespass* ini dibagi lagi ke dalam spam e-mail, web hacking, dan *breaking to PC*. Intinya, masuk ke dalam wilayah pribadi seseorang tanpa izin; dan
3. Ketiga, adalah *cyber terorism*. Terorisme maya (*cyber terorism*) berdimensi luas, tetapi semua menyangkut isu-isu terorisme, mulai dari sekadar pemanfaatan jasa internet untuk berkomunikasi melakukan tindak kejahatan terorisme, hingga pemanfaatan langsung jaringan maya untuk melakukan teror publik.

Menurut NCIS Inggris, sebagaimana dikutip oleh Ade Maman Suherman, menyatakan bahwa manifestasi dari tindak pidana *cybercrime* muncul dalam berbagai macam atau varian sebagai berikut:²⁶

1. *Recreational Hackers*

Kejahatan ini dilakukan oleh netter tingkat pemula untuk sekadar mencoba kekuranghandalan sistem sekuritas suatu perusahaan;

2. *Crackers atau criminal minded hackers*

Pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase, dan penghancuran data. Sebagai contoh, pada tahun 1994 Citibank AS kebobolan senilai 400.000 dolar oleh cracker dari Rusia yang akhirnya dijatuhi hukuman penjara selama tiga tahun serta harus mengembalikan sejumlah uang tersebut. Tipe kejahatan ini dapat terjadi dengan bantuan orang dalam, biasanya staf yang sakit hati atau datang dari kompetitor dalam bisnis sejenis;

3. *Political Hackers*

Aktivitas politik atau lebih populer dengan sebutan *hactivist* melakukan perusakan terhadap ratusan situs web untuk mengkampanyekan program-programnya,

²¹ Widodo, "Aspek Hukum Kejahatan Mayantara", Aswindo, Yogyakarta, 2011, h. 7.

²² Agus Rahardjo, "Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi", Citra Aditya Bakti, Bandung, 2002, h. 32.

²³ Ibid.

²⁴ Abdul Wahid dan Mohamd Labib, "Kejahatan Mayantara (cybercrime)", Bandung, Refika Aditama, 2015, h. 23.

²⁵ Sutanto, Hermawan Sulistiyo, dan Tjuk Sugiarto, "Cyber Crime-Motif dan Penindakan", Pensil, Jakarta, 2005, h. 21.

²⁶ Ade Maman Suherman, "Aspek Hukum Dalam Ekonomi Global", Ghalia Indonesia, Jakarta, 2002, h. 168.

bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendeskreditkan lawannya. Usaha tersebut pernah dilakukan secara aktif dan konsisten dalam usaha untuk kampanye anti – Indonesia dalam masalah Timor Timor yang dipelopori oleh Ramos Horta. Situs Deplu (departemen luar negeri) sempat mendapat serangan yang diduga keras dari kelompok anti integrasi;

4. *Denial of Service Attack*

Serangan *denial of service attack* atau oleh FBI dikenal dengan istilah “*unprecedented*” tujuannya adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna yang legitimate. Taktik yang digunakan adalah dengan mengirim atau membanjiri situs web dengan data yang tidak perlu. Pemilik situs web menderita kerugian karena untuk mengendalikan atau mengontrol kembali situs web memakan waktu yang tidak sedikit; dan

5. *Insiders atau Internal Hackers*

Insider hackers ini bisa dilakukan oleh orang dalam perusahaan sendiri. Modus operandinya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan. Departemen Perdagangan dan Industri Inggris mengumumkan bahwa pada tahun 1998 ada banyak perusahaan-perusahaan yang telah menderita kerugian senilai 1,5 miliar poundsterling.

Unsur-Unsur Tindak Pidana Dalam Cybercrime

Pembobolan *website* digolongkan sebagai kejahatan dibidang informasi dan transaksi elektronik dapat dilihat dari perbuatan yang dilarang dalam Pasal 32 Undang-Undang Nomor 19 Tahun 2016 Tentang perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik menyebutkan :

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

Berdasarkan asas yang berlaku dalam hukum pidana, maka tidak ada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam Peraturan Perundang-Undangan yang telah ada sebelum perbuatan itu dilakukan dalam Pasal 1 Ayat (1) KUHP.²⁷ Sekalipun perkembangan mutakhir dalam hukum pidana menunjukkan bahwa asas hukum tersebut tidak lagi diterapkan secara rigid atau kaku, tetapi asas hukum tersebut sampai sekarang tetap dipertahankan sebagai asas yang sangat fundamental dalam hukum pidana sekalipun dengan berbagai modifikasi dan pengembangan. Dengan demikian seseorang hanya dapat dipersalahkan melakukan tindak pidana apabila orang tersebut melakukan perbuatan yang telah dirumuskan dalam ketentuan undang-undang sebagai tindak pidana.²⁸ Sejauh mana seseorang melakukan perbuatan yang telah dirumuskan dalam undang-undang sebagai tindak pidana dapat dipersalahkan melakukan tindak pidana.

Lazimnya Jawaban normatif yang diberikan oleh hukum pidana berdasarkan asas legalitas seperti tersebut di atas adalah, bahwa seseorang hanya dapat dipersalahkan sebagai telah melakukan tindak pidana apabila orang tersebut oleh hakim telah dinyatakan terbukti bersalah dengan memenuhi unsur-unsur dari tindak pidana yang bersangkutan, seperti yang dirumuskan di dalam undang-undang. Dengan kata lain dapat dikemukakan, bahwa seseorang tidak dapat dipersalahkan melakukan tindak pidana apabila salah satu unsur tindak pidana yang didakwakan kepada orang tersebut tidak dapat dibuktikan.

Sementara itu berkaitan dengan persoalan kemampuan bertanggung jawab ini pembentuk KUHP berpendirian, bahwa setiap orang dianggap mampu bertanggung jawab. Konsekuensi dari pendirian ini adalah, bahwa masalah kemampuan bertanggung jawab ini tidak perlu dibuktikan adanya di pengadilan kecuali apabila terdapat keragu-raguan terhadap unsur tersebut.

Bertolak dari pendirian pembentuk KUHP di atas, dapat dimengerti di dalam KUHP sendiri tidak ada penjelasan tentang apa yang dimaksud dengan kemampuan bertanggung jawab. KUHP hanya memberikan rumusan secara negatif atas kemampuan bertanggung jawab ini terdapat di dalam ketentuan Pasal 44 KUHP yang menyatakan kapan seseorang tidak dapat dipertanggungjawabkan atas perbuatannya.

²⁷ Moelyatno, “Asas-asas Hukum Pidana”, Rineka Cipta, Jakarta, 2000, h. 1.

²⁸ Barda Nawawi Arief, “Bunga Rampai Kebijakan Hukum Pidana”, Citra Aditya Bakti, Bandung, 1996, h. 88.

Dasar pemikiran lain adalah urgensi penggunaan hukum pidana dalam penanggulangan *cybercrime*, jika kriminalisasi suatu perbuatan pidana. Menurut Prof. Nigel Weker, ada beberapa hal yang diperhatikan antara lain:²⁹

- a. Kerugian suatu tindak pidana harus jelas termasuk korbannya harus jelas;
- b. Penegakan hukum (*law an forcement*) harus mendapatkan dukungan masyarakat luas dan dilakukan secara efektif; dan
- c. Kerugian yang timbul karena pemindahan ini harus lebih kecil dari padacakibat tindak pidana.

Unsur melawan hukum Pasal 1365 KUHP data adalah unsur sangat penting dalam kejahatan *cyber*, sudah barang tentu akan menimbulkan kerugian ekonomis pihak lain akibat dari perbuatannya.

Pengertian Carding

Carding adalah modus kejahatan yang dilakukan oleh pelaku yaitu dengan cara menggunakan kartu kredit korban untuk melakukan transaksi.³⁰ Hal ini dapat terjadi dikarenakan pelaku kejahatan mengetahui nomor kartu kredit korbannya. Kejahatan carding ini biasanya dilakukan dengan sistem online melalui situs *e-commerce*. Seperti yang diketahui bahwa saat proses transaksi belanja di *e-commerce*, pelanggan hanya perlu memasukkan nomor digit kartu kredit.

Hal itu yang digunakan oleh pelaku kejahatan untuk melakukan pembobolan kartu kredit tanpa harus memerlukan kartunya secara fisik, pelaku hanya memerlukan nomor dan masa berlakunya kartu kredit tersebut. *Carding* merupakan kejahatan menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan kartu kredit orang lain sehingga dapat merugikan orang tersebut baik materiil maupun nonmateriil.³¹

Website defacement disebut juga web defacement ialah tindakan seseorang tanpa hak mengubah tampilan halaman website dengan cara yang tidak semestinya. Rogmana dan Hout memberikan pendapat bahwa serangan perusakan web berpotensi karena memerlukan biaya untuk memperbaikinya. Dengan studi kasus pada website pemerintah, khususnya yang berdomain .go.id, penelitian ini berfokus pada monitoring serangan *web defacement* agar pemerintah memperhatikan pendanaan setelah membuat sistem berbasis web.³²

Situs web atau *website* adalah salah satu sarana penting yang bisa dimanfaatkan oleh bisnis maupun individu untuk berbagai tujuan. Baik untuk perusahaan kecil, perusahaan besar, maupun *freelancer*, *website* bisa menjadi senjata efektif untuk memperkenalkan diri Anda di internet. Website adalah kumpulan halaman web atau 'lokasi' di internet tempat Anda menyimpan informasi dan menyajikannya agar bisa diakses oleh siapa pun secara online. Informasi ini bisa tentang diri Anda, bisnis, atau bahkan topik yang Anda minati.³³ Seperti 'lokasi' pada umumnya, *website* bekerja menggunakan sistem alamat yang akan memberitahukan lokasi tepatnya di internet sehingga Anda bisa mengaksesnya melalui web browser.

Penjelasan mudahnya, alamat tersebut mirip seperti alamat yang Anda gunakan untuk menuju suatu tempat di aplikasi maps. Ketika Anda mengakses alamat situs, web browser akan menuju ke lokasi yang ditentukan dan mengambil file situs tersebut. Proses pengambilan informasi ini dilakukan oleh layanan web menggunakan teknologi seperti *Hypertext Transfer Protocol* (HTTP) dan *File Transfer Protocol* (FTP). Protokol ini pada dasarnya berfungsi untuk menentukan cara informasi dan file ditransmisikan melalui web.³⁴

Browser kemudian menampilkan halaman tersebut di layar perangkat Anda menggunakan teknologi seperti *HyperText Markup Language* (HTML) dan *Cascading Style Sheet* (CSS). Teknologi ini menyusun dan menyajikan isi website kepada pengunjung dengan memberi tahu web browser tentang posisi penyajian informasi yang benar di layar. Meskipun membutuhkan bahasa pemrograman atau coding agar website bisa ditampilkan di layar, untungnya Anda tidak perlu mempelajari bahasa pemrograman atau memiliki latar belakang di bidang IT untuk membuat website.

PERTANGGUNGJAWABAN HUKUM TERHADAP TINDAK PIDANA PENGAKSESAN KARTU KREDIT TANPA HAK DENGAN SISTEM PERETASAN MELALUI WEBSITE

Pertanggung jawaban Hukum Pidana

Pertanggung jawaban (hukum) berasal dari kata dasar "tanggung" dan "jawab". Secara umum tanggung jawab hukum dapat diartikan sebagai suatu konsekuensi hukum yang timbul sebab adanya suatu

²⁹ Robintan Sulaiman, "Cyber Crimes (Perspektif E-Commerce Crime)", Cet. I, Universitas Pelita Harapan, Jakarta, 2002, h. 90.

³⁰ Nudirman Munir, "Pengantar Hukum Siber Indonesia", Rajawali Pers, Depok, 2017, h. 230.

³¹ *Ibid.*

³² Fazlurrahman, Dedy Haryadi, "Analisis Serangan Web Defacement pada Situs Web Pemerintah Menggunakan

ELK Stack", JISKa, Vol. 4, No. 1, Mei, Universitas Jenderal Ahmad Yani, Yogyakarta, 2019, h. 2.

³³ Developer Web, "Pengertian website dan jenisnya", https://www.hostinger.co.id/tutorial/website-adalah#Pengertian_Website, Online diakses pada 10 Juni 2024 pukul 20.30.

³⁴ *Ibid.*

kesalahan (kesengajaan ataupun kelalaian) maupun tanpa adanya suatu kesalahan.³⁵ Umumnya konsep tanggung jawab hukum akan merujuk kepada tanggung jawab dalam bidang Hukum Privat (tanggung jawab perdata), dan tanggung jawab dalam Hukum Publik (misalnya tanggung jawab pidana maupun administrasi).

Strict liability merupakan salah satu jenis konsep pertanggung jawaban hukum. Di Indonesia, istilah yang sering digunakan untuk merujuk pada *strict liability* adalah “pertanggung jawaban risiko”, “pertanggung jawaban tanpa perlu pembuktian unsur kesalahan”, atau “pertanggung jawaban secara ketat”.³⁶ Dasar dari pertanggung jawaban bukan lagi perbuatannya memenuhi atau tidak memenuhi unsur kesalahan, tetapi mengenai pelaku telah terlibat dalam suatu kegiatan berbahaya yang dapat menimbulkan kerugian. Dengan telah terlibatnya pelaku dalam perbuatan yang berbahaya, maka pelaku yang bertanggung jawab atas kerugian yang timbul karena bahaya tersebut tanpa melihat mengenai melawan hukum atau tidaknya perbuatan tersebut.³⁷

Konsep tanggung jawab dikemukakan oleh pencetus teori hukum murni yaitu Hans Kelsen. Menurut Hans, tanggung jawab berkaitan erat dengan kewajiban, namun tidak identik. Kewajiban tersebut muncul karena adanya aturan hukum yang mengatur dan memberikan kewajiban kepada subjek hukum. Subjek Hukum yang dibebani kewajiban harus melaksanakan kewajiban tersebut sebagai perintah dari aturan hukum.

Akibat dari tidak dilaksanakannya kewajiban maka akan menimbulkan sanksi. Sanksi ini merupakan tindakan paksa dari aturan hukum supaya kewajiban dapat dilaksanakan dengan baik oleh subyek hukum. Menurut Hans, subyek hukum yang dikenakan sanksi tersebut dikatakan “bertanggung jawab” atau secara hukum bertanggung jawab atas pelanggaran.³⁸ Berdasarkan konsep tersebut, maka dapat dikatakan bahwa tanggung jawab muncul dari adanya aturan hukum yang memberikan kewajiban kepada subyek hukum dengan ancaman sanksi apabila kewajiban tersebut tidak dilaksanakan. Tanggung jawab demikian dapat juga dikatakan sebagai tanggung jawab hukum, karena muncul dari

perintah aturan hukum/ undang-undang dan sanksi yang diberikan juga merupakan sanksi yang ditetapkan oleh undang-undang, oleh karena itu pertanggung jawaban yang dilakukan oleh subyek hukum merupakan tanggung jawab hukum.

Pertanggungjawaban Pidana Terhadap Pelaku Kejahatan Carding

Pertanggungjawaban pidana dalam bahasa Inggris disebut sebagai *criminal liability* atau *responsibility* yang menjurus kepada kepidanaan.³⁹ Bahwa pertanggungjawaban pidana dimaksudkan untuk menentukan apakah seorang tersangka/terdakwa dipertanggungjawabkan untuk menanggung konsekuensi atas perbuatannya karena telah melakukan suatu kejahatan yang merugikan.

Pesatnya teknologi informasi melalui internet telah mengubah aktivitas- aktivitas kehidupan yang semula perlu dilakukan secara kontak fisik, kini dengan menggunakan media *cyberspace*, aktivitas keseharian dapat dilakukan secara virtual atau maya. Masalah rumit yang dihadapi penegak hukum saat ini adalah bagaimana menjangkit pelaku *cybercrime* yang mengganggu rasa keadilan tersebut dikaitkan dengan ketentuan pidana yang berlaku.⁴⁰ KUHP tidak mampu mengkoordinir segala bentuk kejahatan yang sudah berkembang pesat. Hal ini karena KUHP merupakan produk lama sementara *cybercrime* merupakan dunia masa kini yang mengandalkan teknologi tinggi.

Pertanggungjawaban pidana merupakan diteruskannya celan obyektif yang ada pada tindak pidana, dan secara subyektif kepada seorang yang memenuhi syarat untuk dapat dijatuhi pidana karena perbuatannya.⁴¹ Dengan perkataan lain apakah terdakwa akan dipidana atau dibebaskan. Jika ia dipidana, harus nyata bahwa tindakan yang dilakukan itu bersifat melawan hukum dan terdakwa mampu bertanggungjawab. Kemampuan tersebut memperhatikan kesalahan dari petindak yang berbentuk kesengajaan atau kealpaan.⁴² Pertanggungjawaban atau yang dikenal dengan konsep *liability* dalam segi falsafah hukum. Roscoe Pound menyatakan bahwa pertanggungjawaban pidana diartikan sebagai suatu kewajiban untuk membayar pembalasan yang akan diterima pelaku dari seseorang yang telah dirugikan.⁴³ Untuk dapat

³⁵ Rony Andre Christian Naldo, dkk, “Penerapan Pertanggungjawaban Mutlak Sebab Perbuatan Melawan Hukum Mengakibatkan Kerugian Lingkungan Hidup”, Nas Media Pustaka, Makassar, 2022, h. 82.

³⁶ *Ibid*, h. 82.

³⁷ *Ibid*, h. 51.

³⁸ Hans Kelsen, “Pure Theory of Law, Terjemah, Raisul Muttaqien, Teori Hukum Murni: Dasar-Dasar Ilmu Hukum Normatif”, Cetakan Ke VI, Penerbit Nusa Media, Bandung, 2008, h. 136.

³⁹ Erni Juniria Harefa.dkk, “Pertanggungjawaban Pidana Korporasi (PT) Atas Tindak Pidana Perusakan

Lingkungan Hidup”, Jurnal Magister Hukum Program Pascasarjana Universitas HKBP Nommensen, Vol. 2, No. 2, Medan, 2021, h. 147.

⁴⁰ *Ibid*.

⁴¹ *Ibid*.

⁴² E.Y. Kanter dan S.R. Sianturi, “Asas-Asas Hukum Pidana Di Indonesia Dan Penerapannya”, Stora Grafika, Jakarta, 2002, h. 250.

⁴³ Romli Atmasasmita, “Perbandingan Hukum Pidana”, Mandar Maju, Bandung, 2000, h. 65.

dipidananya si pelaku, diharuskan tindak pidana yang dilakukannya itu memenuhi unsur-unsur delik yang telah ditentukan dalam undang-undang.

Apabila diterjemahkan delik merupakan perbuatan yang dapat dikenakan hukuman karena merupakan pelanggaran terhadap undang-undang atau delik juga disebut sebagai tindak pidana. Namun untuk saat ini kata tindak pidana lebih sering disebut dengan delik karena banyak ahli/penulis menerjemahkan kata delik dengan istilah yang berbeda namun memiliki arti yang sama. Untuk itu, disetiap tulisan memakai kata delik saja, yang netral itu.⁴⁴ Pertanggungjawaban pidana merupakan suatu bentuk untuk menentukan apakah seseorang akan dilepas atau dipidana atas tindak pidana yang telah terjadi, dalam hal ini untuk mengatakan bahwa seseorang memiliki aspek pertanggungjawaban pidana maka dalam hal itu terdapat beberapa unsur yang harus terpenuhi untuk menyatakan bahwa seseorang tersebut dapat dimintakan pertanggungjawaban.⁴⁵

Seseorang yang telah melakukan suatu tindak pidana sedapatnya untuk bisa dimintai pertanggungjawabannya secara garis besar harus memenuhi unsur tindak pidana yang telah diperbuat olehnya, serta harus diperhatikan pula kondisi dari pelaku tindak pidana. Menurut Sudarto, bahwa pertanggungjawaban pidana (kesalahan dalam arti yang seluas-luasnya) terdiri atas beberapa unsur yaitu:⁴⁶

- a. Adanya kemampuan bertanggung jawab pada si pembuat, artinya keadaan jiwa si pembuat normal;
- b. Hubungan batin antara si pembuat dengan perbuatannya yang berupa kesengajaan (*dolus*) atau kealpaan (*culpa*); dan
- c. Tidak adanya alasan yang menghapus kesalahan atau tidak adanya alasan pemaaf.

Pertanggungjawaban merupakan inti dari kesalahan yang dimaksud dalam hukum pidana. walaupun sebenarnya menurut etika setiap orang bertanggungjawab atas setiap perbuatannya, tetapi dalam hukum pidana yang menjadi pokok permasalahan hanyalah tingkah laku yang mengakibatkan hakim menjatuhkan pidana.⁴⁷

Dalam menegakan hukum pidana atas pertanggung jawaban pidana atas perbuatannya,

Menurut Eddy O.S. Hiariej seseorang harus memenuhi 3 (tiga) syarat yaitu:⁴⁸

- 1) Kemampuan bertanggungjawab;
- 2) Hubungan psikis pelaku dengan perbuatan yang dilakukan; dan
- 3) Tidak ada alasan yang menghapus pertanggungjawaban pidana berupa alasan pemaaf yang menghapuskan sifat melawan hukumnya perbuatan dan alasan pemaaf yang menghapuskan sifat dapat dicelanya pelaku.

Menurut penulis pertanggungjawaban pidana adalah mengenakan hukuman kepada orang atau badan hukum karena perbuatan yang dilarang atau menimbulkan keadaan yang terlarang, karenanya menyangkut proses peralihan hukuman yang ada pada tindak pidana kepada pembuatnya. Pertanggungjawaban pidana ditentukan berdasarkan kesalahan yang ditempatkan sebagai faktor penentu pertanggungjawaban pidana.

Aspek Pembuktian Terhadap Tindak Pidana Carding

Pembuktian dalam hukum pidana merupakan sub sistem kebijakan kriminal sebagai *science of response* yang mencakup berbagai disiplin ilmu. Hal ini disebabkan oleh luasnya kausa dan motif berkembangnya jenis kejahatan yang berbasis teknologi informasi saat ini. Pada hakekatnya, pembuktian dimulai sejak adanya suatu peristiwa hukum. Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan (serangkaian tindakan penyelidikan untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyelidikan menurut cara yang diatur dalam undang-undang ini), yang diatur dalam dalam pasal 1 angka 13 Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian.

Menurut M.Yahya Harahap, pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa.⁴⁹ Menurut Pitlo, “pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya”.⁵⁰

⁴⁴ Amdi Hamzah, “Asas-Asas Hukum Pidana”, Rineka Cipta, Jakarta, 2010, h. 94.

⁴⁵ Antoni Arapenta.dkk, “Pertanggungjawaban Pidana Warga Negara Asing Yang Masuk Ke Wilayah Indonesia Tanpa Dokumen Perjalanan”, PATIK – Jurnal Hukum, Vol. 7, No. 3, 2018, h. 3.

⁴⁶ Adhyaksa Mahasena, “Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Jual Beli Organ Tubuh Manusia”, Jurnal Hukum Vol. 7 No, Universitas Udayana, Bali, 2018, h. 80.

⁴⁷ Teguh Prasetyo, “Hukum Pidana”, Raja Grafindo Persada, Depok, 2017, h. 78.

⁴⁸ Eddy O.S. Hiariej, “Prinsip-Prinsip Hukum Pidana”, Cahaya Atma Pustaka, Yogyakarta 2014, h. 93.

⁴⁹ M. Yahya Harahap, “Pembahasan Permasalahan dan Penerapan KUHAP: penyidik dan penuntutan”, Cet. 2, Sinar Grafika, Jakarta, 2010, h. 73.

⁵⁰ Edmon Makarim, “Kompilasi Hukum Telematika”, Raja grafindo Persada, Jakarta, 2003, h. 417.

Menurut Subekti, yang dimaksudkan dengan “membuktikan” adalah meyakinkan hakim tentang kebenaran dalil ataupun dalil-dalil yang dikemukakan oleh para pihak dalam suatu persengketaan.⁵¹ “Pembuktian tentang benar tidaknya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting dalam hukum acara pidana”. Berhadapan dengan kasus *cybercrime*, pembuktian menjadi masalah yang pelik. Seringkali penegak hukum di Indonesia mengalami kesulitan saat menjerat pelaku *cybercrime* karena masalah pembuktian (*documentary evidence*) yang tidak memenuhi ketentuan sistem hukum pidana Indonesia. Sementara upaya penjeratan terhadap pelaku-pelaku *cybercrime* harus tetap dilakukan, upaya perluasan menjadi solusi untuk menegakan hukum.

Hukum pembuktian merupakan sebagian dari hukum pidana yang mengatur tentang alat-alat bukti yang sah menurut hukum, barang-barang bukti, sistem pembuktian yang dianut, syarat dan tata cara pembuktian yang dilakukan, serta kewenangan hakim untuk menerima, menolak dan menilai suatu pembuktian.⁵² Sumber hukum pembuktian adalah undang-undang, doktrin dan *jurisprudensi*. Oleh karena itu, Undang-undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana (KUHP) menjadi salah satu sumber hukum dalam proses pembuktian.

Pembuktian merupakan titik sentral pemeriksaan perkara dalam sidang pengadilan. Pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang untuk membuktikan kesalahan yang didakwakan kepada terdakwa. Pembuktian juga merupakan ketentuan yang mengatur alat-alat bukti yang dibenarkan undang-undang yang dapat dipergunakan hakim dalam membuktikan kesalahan terdakwa. Oleh karena itu, hakim tidak dapat mempergunakan alat bukti yang bertentangan dengan undang-undang. Kebenaran atas suatu putusan harus teruji dengan alat bukti yang sah secara hukum serta memiliki kekuatan pembuktian yang melekat pada setiap alat bukti yang ditemukan.

Pertanggungjawaban Tindak Pidana Carding Undang-Undang Nomor 19 Tahun 2016 Tentang perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Hukum pidana pada prinsipnya bertujuan untuk memberikan rasa keadilan bagi seluruh masyarakat Indonesia. Dengan demikian, Hukum pidana mengatur segala sesuatu yang berhubungan dengan perbuatan pidana. Dalam hukum pidana,

seseorang yang melakukan kejahatan akan diberikan sanksi atau hukuman sesuai dengan perbuatan pidananya. Hal ini bermaksud agar pelaku tindak pidana akan merasakan efek jera dan tidak akan mengulangi perbuatannya. Selain itu, dengan adanya penerapan sanksi pidana, diharapkan adanya efek pembelajaran bagi masyarakat umum agar tidak melakukan tindak pidana. Sebagaimana yang telah dijabarkan sebelumnya bahwa *carding* mengacu pada sebuah transaksi elektronik yang melibatkan proses jual-beli dengan menggunakan kartu kredit yang tidak sah.⁵³

Sah atau tidaknya dari proses transaksi kartu kredit yang dimaksud adalah proses *autentifikasi* dan otorisasi pengguna kartu kredit. Proses *autentifikasi* dan otorisasi dari pengguna kartu kredit itu sendiri mengacu pada kepemilikan dari kartu kredit. Seseorang yang memiliki kartu kredit seharusnya mempunyai kemampuan memberikan data pribadi dalam proses *autentifikasi* dan otorisasi kartu kredit. Namun demikian, sebagian orang dengan kemampuan teknis dapat mencuri data pribadi pemilik kartu kredit dan menggunakan data tersebut seolah-olah orang tersebut pemilik sah dari kartu kredit yang digunakan. Pemerintah Indonesia mengatur tindak pidana yang menggunakan transaksi elektronik dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 yang kemudian di Amandemen dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Dalam Pasal 32 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik khususnya pada, diatur tentang pencurian data/informasi elektronik dengan bunyi sebagai berikut :“Setiap orang dengan sengaja dan tanpa hak tau melawan hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak.”

Dari kutipan diatas dapat kita pahami bahwa unsur memindahkan suatu barang dari satu tempat ke tempat lain tanpa hak atau persetujuan dari orang yang memilikinya merupakan sebuah bentuk pencurian sebagaimana juga yang dijelaskan pada Pasal 362 KUHP.⁵⁴

Sedangkan benda yang merujuk kepada segala sesuatu yang berwujud maupun tidak berwujud dan mempunyai nilai dalam kehidupan ekonomi seseorang dalam konteks ini adalah informasi elektronik dan atau dokumen elektronik. Dalam hal pengaturan sanksi pidana dalam Pasal 48 ayat (2)

Modus carding menurut Undang-Undang Informasi dan Transaksi Elektronik”, Jurnal Artikel Skripsi, Fakultas hukum Universitas Sam Ratulangi, Manado, h. 2.

⁵⁴ *Ibid.*

⁵¹ Subekti, “*Hukum Pembuktian*”, Pradnya Paramita, Jakarta, 1995, h. 1.

⁵² *Ibid.*

⁵³ Hizkia Eliezer Malalang, “*Pertanggungjawaban Pidana pelaku Pembobolan Kartu Kredit dengan*

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik sebagaimana tertulis: “Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (Sembilan) tahun dan/atau denda paling banyak Rp 3.000.000.000 (tiga miliar rupiah).” Kejahatan dalam ruang *cyber* bersifat transnasional dimana kejahatan ini dapat terjadi secara lintas batas wilayah negara tetapi akibatnya memiliki implikasi hukum di Indonesia.⁵⁵ Dengan demikian perlu adanya penentuan yurisdiksi apabila *cybercrime* yang terjadi nantinya bersifat lintas batas negara.

Yurisdiksi adalah kekuasaan atau kompensasi hukum negara terhadap orang, benda ataupun peristiwa hukum. Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak campur tangan. Yurisdiksi merupakan suatu bentuk kedaulatan vital dan sentral yang dapat mengubah, menciptakan, atau mengakhiri suatu hubungan atau kewajiban hukum.

PENUTUP

Kesimpulan

Belum adanya pembatasan hukum terhadap pengaksesan informasi maupun tindakan melalui internet menjadi akses ilegal terhadap sistem komputer, ini membuat keseluruhan kegiatan *hacking* maupun *cracking* merupakan suatu bentuk tindak pidana kejahatan dunia maya (*cybercrime*). Pengaturan Tindak Pidana *Hacking* dan *cracking*. Pengaturan tindak pidana *Hacking* dirumuskan pada Pasal 32 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. bahwa pada dasarnya tindak pidana *hacking* maupun *cracking* merupakan suatu tindakan setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik orang lain dengan tujuan memperoleh informasi dan/atau dokumen elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Terhadap batasan informasi maupun akses lainnya masih tergantung kepada sistem pengamanan tiap website itu sendiri.

Pertanggungjawaban pidana pelaku kejahatan *hacking* dan *cracking* tertuang dalam Pasal 48 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik menyebutkan : “Setiap Orang yang memenuhi unsur

sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah)”.

Saran

1. Mengingat dampak yang ditimbulkan tindak pidana *hacking* dan *cracking* sangat berbahaya bagi *privasi* seseorang maupun instansi atau lembaga hukum maka hendaknya pemilik situs atau *website* memberikan pengamanan *software* komputer baik berupa penggunaan *firewall*, mengunci data dengan *password* yang tidak mudah di akses, *mem-backup* data secara rutin dan berkala, dan berbagai macam pengamanan lainnya.
2. Pemerintah melalui Menteri Komunikasi dan Informatika perlu mengeluarkan aturan main *hacking* dan *cracking* dengan mengeluarkan peraturan pemerintah selain untuk menjelaskan beberapa pasal yang masih mengambang (salah perspektif), selain itu agar tindak pidana *hacking* dapat diatur secara lebih rinci dan memperjelas tindakan-tindakan apa saja yang di kemudian hari dapat berpotensi sebagai tindak pidana *hacking* maupun *cracking*. juga untuk memudahkan bagi profesional yang bergerak dalam bidang teknologi informasi, serta memberikan pendidikan kepada masyarakat melalui peraturan yang ada. Sehingga aktivitas mereka tetap terlindungi hukum. Juga terhadap para penegak hukum sebaiknya lebih meningkatkan kualitas aparaturnya dalam bidang teknologi informasi.

UCAPAN TERIMA KASIH

Dengan terselesaikannya penelitian ini, penulis mengucapkan terima kasih kepada bapak ibu guru yang telah membimbing penuh kesabaran dan ketabahan, tak lupa juga kepada orang tua tercinta. ibu dan ayah, yang memberikan kasih sayang dan doa tak henti-hentinya untuk selalu mendukung kemajuan anak-anaknya, dan semoga Allah SWT selalu memberikan kasih sayang kepada mereka di dunia dan akhirat. Serta kepada teman-teman Fakultas Hukum Universitas Gresik angkatan 2020 atas kebersamaannya selama menempuh pendidikan dan berbagi pengetahuan. Semua pihak yang tidak dapat disebutkan satu persatu. Semoga segala bantuan yang diberikan kepada penulis mendapatkan pahala oleh Tuhan Yang Maha Esa. Akhir kata penulis menyadari bahwa skripsi ini masih belum sempurna namun besar harapan penulis semoga tulisan ini dapat berguna dan bermanfaat untuk kita semua, terlebih untuk

⁵⁵ Didik M.Arief Mansur, “*Cyber Law-Aspek Hukum Teknologi Informasi*”, Refika Aditama, Bandung, 2005, h. 30.

pihakpihak yang membutuhkan sebagai bahan rujukan atau referensi dikemudian hari. Aamiin.

DAFTAR PUSTAKA

Buku-buku

- Arief, Barda Nawawi, "*Bunga Rampai Kebijakan Hukum Pidana*", Citra Aditya Bakti, Bandung, 1996.
- Arief, Barda Nawawi, "*Kapita Selekta Hukum Pidana*", Citra Aditya Bakti, Bandung, 2003
- Arief, Barda Nawawi, "*Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*", PT Raja Grafindo Persada, Jakarta, 2007.
- Atmasasmita, Romli, "*Perbandingan Hukum Pidana*", Mandar Maju, Bandung, 2000.
- Barakatullah, Abdul Halim, Teguh Prasetyo, "*Bisnis E-Commerce Studi System Keamanan dan Hukum di Indonesia*", Pustaka Pelajar, Yogyakarta, 2006.
- Hamzah, Amdi, "*Asas-Asas Hukum Pidana*", Rineka Cipta, Jakarta, 2010.
- Harahap, M. Yahya, "*Pembahasan Permasalahan dan Penerapan KUHAP: penyidik dan penuntutan*", Cet. 2, Sinar Grafika, Jakarta, 2010.
- Kanter, E.Y. dan S.R. Sianturi, "*Asas-Asas Hukum Pidana Di Indonesia Dan Penerapannya*", Stora Grafika, Jakarta, 2002.
- Kelsen, Hans, "*Pure Theory of Law, Terjemah, Raisul Muttaqien, Teori Hukum Murni: Dasar-Dasar Ilmu Hukum Normatif*", Cetakan Ke VI, Penerbit Nusa Media, Bandung, 2008.
- Kristian dan Yopi Gunawan, "*Sekelumit tentang Penyadapan dalam Hukum Positif di Indonesia*", Nuansa Aulia, Bandung, 2013.
- M. Echols, John dan Hassan Shadily, "*Kamus Inggris-Indonesia Cet. XXV*"; Gramedia Pustaka Utama, Jakarta, 2003.
- Makarim, Edmon, "*Kompilasi Hukum Telematika*", Raja grafindo Persada, Jakarta, 2003.
- Malalang, Hizkia Eliezer, "*Pertanggungjawaban Pidana pelaku Pembobolan Kartu Kredit dengan Modus carding menurut undang-Undang Informasidan Transaksielektronik*", Jurnal Artikel Skripsi, Fakultas hukum Universitas Sam Ratulangi, Manado.
- Mansur, Didik M. Arief, "*Cyber Law-Aspek Hukum Teknologi Informasi*", Refika Aditama, Bandung, 2005.
- Maskun, "*Kejahatan Siber Cyber Crime*", Kencana, Jakarta, 2013.
- Moelyatno, "*Asas-asas Hukum Pidana*", Rineka Cipta, Jakarta, 2000.
- Munir, Nudirnan, "*Pengantar Hukum Siber Indonesia*", Rajawali Pers, Depok, 2017.
- Naldo, Rony Andre Christian, dkk, "*Penerapan Pertanggungjawaban Mutlak Sebab Perbuatan Melawan Hukum Mengakibatkan Kerugian Lingkungan Hidup*", Nas Media Pustaka, Makassar, 2022.
- O.S. Hiariej, Eddy, "*Prinsip-Prinsip Hukum Pidana*", Cahaya Atma Pustaka, Yogyakarta 2014.
- Prasetyo, Teguh, "*Hukum Pidana*", Raja Grafindo Persada, Depok, 2017.
- Rahardjo, Agus, "*Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*", Citra Aditya Bakti, Bandung, 2002.
- Subekti, "*Hukum Pembuktian*", Pradnya Paramita, Jakarta, 1995.
- Suherman Ade Maman, "*Aspek Hukum Dalam Ekonomi Global*", Ghalia Indonesia, Jakarta, 2002.
- Sulaiman, Robintan, "*Cyber Crimes (Perspektif E-Commerce Crime)*", Cet. I, Universitas Pelita Harapan, Jakarta, 2002.
- Sulistiyo Sutanto, Hermawan, dan Tjuk Sugiarto, "*Cyber Crime-Motif dan Penindakan*", Pensil, Jakarta, 2005.
- Suyanto, "*Metode Penelitian Hukum Pengantar Penelitian Normatif, Empiris dan Gabungan*", Unigres Press, Gresik, 2023.
- , "*Pengantar Hukum Pidana*", Ed.1, Cet.1, Deepublish, Yogyakarta, 2018.
- , "*Hukum Acara Pidana*", Cet.1, Zifatama Jawara, Sidoarjo, 2018.
- Wahid, Abdul dan Mohamd Labib, "*Kejahatan Mayantara (cybercrime)*", Bandung, Refika Aditama, 2015.
- Widjojo, Widyopramono Hadi, "*Cybercrimes dan Pencegahannya*", jurnal Hukum Teknologi, Fakultas Hukum Universitas Indonesia, Jakarta, 2005.
- Widodo, "*Aspek Hukum Kejahatan Mayantara*", Aswindo, Yogyakarta, 2011.

Jurnal

- Arapenta, Antoni.dkk, "*Pertanggungjawaban Pidana Warga Negara Asing Yang Masuk Ke Wilayah Indonesia Tanpa Dokumen Perjalanan*", PATIK – Jurnal Hukum, Vol. 7, No. 3, 2018.
- Arief M, Zainal, "*Tinjauan Yuridis Penyalahgunaan Kartu Debit Sebagai Tindak Pidana Informasi Dan Transaksi Elektronik (Studi Kasus Putusan Nomor. 1985/Pid.B/2012/PN.MKS)*", Skripsi, Sarjana Hukum, Fakultas Hukum Universitas Hasanuddin, Makassar, 2016.
- Astomo, Putera, "*Prinsip-Prinsip Negara Hukum Indonesia Dalam UUD NRI Tahun 1945*", Jurnal Hukum, Ilmu Hukum FISIP

UNSULBAR, Vol. 1, Nomor 1 Januari, Universitas Sulawesi Barat, 2017.

Fazlurrahman, Dedy Haryadi, “*Analisis Serangan Web Defacement pada Situs Web Pemerintah Menggunakan ELK Stack*”, JISKa, Vol. 4, No. 1, Mei, Universitas Jenderal Ahmad Yani, Yogyakarta, 2019.

Harefa, Erni Juniria dkk, “*Pertanggungjawaban Pidana Korporasi (PT) Atas Tindak Pidana Perusakan Lingkungan Hidup*”, Jurnal Magister Hukum Program Pascasarjana Universitas HKBP Nommensen, Vol. 2, No. 2, Medan, 2021.

Mahasena, Adhyaksa, “*Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Jual Beli Organ Tubuh Manusia*”, Jurnal Hukum Vol. 7 No, Universitas Udayana, Bali, 2018.

Zuraida, Mehda. “*Credit Card Fraud (Carding) dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia*”, Jurnal Analisis Hubungan Internasional, Vol. 4. No. 1. Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Airlangga, Surabaya, 2015.

Media Internet

Ancaman Hacker Website, “*Hacker Selalu Menjadi Ancaman Serius Bagi Keamanan Berbagai Kegiatan*”, <https://thidiweb.com/ancaman-hacker-website/>, Online diakses pada 13 Desember 2023, pukul 19.23.

Developer Web, “*Pengertian website dan jenisnya*”, https://www.hostinger.co.id/tutorial/website-adalah#Pengertian_Website, Online diakses pada 10 Juni 2024 pukul 20.30.

Peraturan Perundang-undangan

Undang-Undang Dasar Tahun 1945;

Kitab Undang-Undang Hukum Perdata;

Kitab Undang-Undang Hukum Pidana;

Undang-Undang Nomor 19 Tahun 2016 Tentang

Perubahan Atas Undang-Undang Nomor 11 Tahun

2008 Tentang Informasi Dan Transaksi Elektronik;

Peraturan Bank Indonesia Nomor 14/2/PBI/2012

perihal Perubahan atas Peraturan Bank Indonesia

Nomor 11/11/PBI/2009 tentang Penyelenggaraan

Kegiatan Alat Pembayaran; dan

Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang

Perdagangan Melalui Sistem Elektronik.

Putusan Pengadilan

Putusan Nomor : 500/Pid.Sus/2019/PN Jkt.Sel