Jurnal Kritis Studi Hukum

Vol. 9 No. 6 Tahun 2024
Halaman 45-53

MENGUNGKAP JEJAK DIGITAL: STUDI KASUS ALAT BUKTI ELEKTRONIK KASUS CARDING DI BALI PADA TAHUN 2023

Dhevanda Ashar Evrast Avrizal[1], Okti Indah Lestari[2]
Dhevandaa@gmail.com[1], oktiindahlestari@gmail.com[2]
Universitas Tidar

Abstrak

Pada tahun 2023 di Bali, di mana MA, seorang pria berusia 41 tahun dari Jakarta Selatan, ditetapkan sebagai pelaku carding oleh Kepolisian Daerah Bali. Carding merupakan tindakan penipuan kartu kredit yang dilakukan secara daring oleh carder untuk memperoleh barang atau dana secara ilegal. Dalam kasus ini, alat bukti elektronik memainkan peran kunci dalam proses penyelidikan dan pembuktian tindak pidana carding. Setelah penyelidikan lebih lanjut, MA dan pacarnya ditangkap di Mall Bali Galeria. Dari pemeriksaan terungkap bahwa MA menggunakan data kartu kredit milik orang lain yang dibeli di Dark Web untuk kegiatan carding. Penggunaan alat bukti elektronik, seperti data dari laptop Macbook MA yang berisi 1.293 data kartu kredit, menjadi kunci dalam mengidentifikasi pelaku dan membuktikan tindak pidana carding. Kasus ini menyoroti pentingnya regulasi hukum terkait cybercrime, seperti Undang-Undang ITE, dalam melindungi informasi elektronik dan menegakkan keadilan dalam kasus kejahatan daring seperti carding dengan menggunakan pendekatan yuridis normatif.
Kata Kunci: Carding, Penipuan, Alat bukti elektronik.

Abstract

In 2023 in Bali, where MA, a 41-year-old man from South Jakarta, was named as a carding offender by the Bali Regional Police. Carding is an act of credit card fraud committed online by carders to illegally obtain goods or funds. In this case, electronic evidence played a key role in the process of investigating and proving the crime of carding. After further investigation, MA and his girlfriend were arrested at Bali Galeria Mall. The investigation revealed that MA used other people's credit card data purchased on the Dark Web for carding activities. The use of electronic evidence, such as data from MA's Macbook laptop containing 1,293 credit card data, was key in identifying the perpetrators and proving the carding crime. This case highlights the importance of legal regulations related to cybercrime, such as the ITE Law, in protecting electronic information and upholding justice in online crime cases such as carding using a normative juridical approach.
Keywords: *carding, fraud, Electronic Evidence.*

PENDAHULUAN

Saat ini, penggunaan internet di Indonesia telah mendekati tingkat yang mengkhawatirkan. Perkembangan kejahatan siber, atau yang disebut cybercrime, adalah konsekuensi dari kemajuan teknologi informasi (TI). Di satu sisi, perkembangan ini menawarkan berbagai kemudahan bagi manusia, tetapi di sisi lain, sering digunakan sebagai sarana untuk melakukan kejahatan siber, seperti yang sering kita lihat akhir-akhir ini. Ancaman cybercrime semakin melonjak, baik terhadap perorangan maupun organisasi atau lembaga pemerintah yang semakin mengandalkan teknologi dan internet.

Perkembangan teknologi informasi dan komunikasi membuka berbagai peluang baru di berbagai sektor, termasuk sektor keuangan. Namun, perkembangan ini juga memberikan

peluang kepada pelaku untuk melakasanakan aksi kejahatan dengan menggunakan teknologi. Salah satu contohnya adalah kejahatan carding, yaitu pencurian informasi kartu kredit yang kemudian digunakan untuk melakukan transaksi tanpa sepengetahuan pemilik kartu.

Dalam salah satu kasus yang diteliti, Direktorat Reserse Kriminal Khusus Kepolisian Daerah Bali berhasil mengamankan pelaku pencurian 1.293 data kartu kredit milik orang lain, yang dikenal sebagai carding. Pelaku bernama MA, berusia 41 tahun, berasal dari Jakarta, dan memakai data kartu kredit yang dicuri guna membeli tiket hotel dan pesawat dengan harga murah.

Dalam kasus carding yang terjadi di Bali ini, alat bukti elektronik menjadi kunci untuk mengidentifikasi pelaku dan membuktikan tindak pidana carding. Bukti elektronik ini diperoleh dari berbagai sumber, termasuk perangkat elektronik yang disita dari pelaku. Dari pemeriksaan laptop MacBook milik MA, ditemukan 1.293 data kartu kredit milik orang lain dari berbagai bank, baik dalam maupun luar negeri, yang telah diretas oleh tersangka MA. Data kartu kredit tersebut didapatkan dengan melakukan pembelian pada situs Dark Web, mendapat harga rata-rata 20 USD per data kartu kredit, yang dibayarkan menggunakan mata uang kripto.

Pengkajian studi kasus ini mempunyai tujuan guna menganalisis peran alat bukti elektronik saat penyelesaian kasus Carding yang terjadi di Bali pada tahun 2023 silam. Selain itu, studi kasus ini dapat membantu meningkatkan kesadaran masyarakat tentang risiko carding dan bagaimana melindungi diri dari kejahatan ini.

Seperti yang telah dijelaskan sebelumnya, "Carding" merujuk pada praktik di mana seseorang menggunakan kartu kredit yang didapatkan secara ilegal untuk melakukan transaksi jual beli secara daring. Keabsahan transaksi tersebut ditentukan oleh apakah proses autentikasi dan otorisasi yang diperlukan telah dipenuhi atau tidak. Dalam hal ini, autentikasi merujuk pada proses verifikasi identitas pemegang kartu kredit, sementara otorisasi adalah proses persetujuan transaksi oleh penerbit kartu kredit. Tanpa kedua proses ini, transaksi dianggap ilegal dan merupakan bagian dari aktivitas kejahatan siber yang dapat merugikan pemilik kartu kredit serta lembaga keuangan terkait.

Pemerintah Indonesia menetapkan aturan mengenai kejahatan yang melibatkan transaksi elektronik dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah dengan UU Nomor 19 Tahun 2016. Dalam Undang-Undang ITE, khususnya pasal 32 ayat (2), diatur tentang pencurian data atau informasi elektronik dengan bunyi:

“Setiap orang dengan sengaja dan tanpa Hak atau melawan hukum dengan caraapapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak.”

Ketentuan ini bertujuan untuk melindungi informasi dan data elektronik dari pencurian, peretasan, dan penyalahgunaan yang dapat merugikan individu maupun perusahaan. Penerapan pasal ini menunjukkan komitmen pemerintah untuk melindungi keamanan siber seiring dengan kemajuan teknologi informasi. Di samping itu, undang-undang ini juga memberikan landasan hukum yang kuat bagi aparat penegak hukum guna menindak pelaku cyber crime, termasuk mereka yang terlibat dalam aktivitas carding.

Untuk memastikan efektifitas penegakan hukum, berbagai lembaga seperti kepolisian, Kementerian Komunikasi dan Informatika, serta Badan Siber dan Sandi Negara (BSSN) bekerja sama dalam memantau dan menindaklanjuti pelanggaran yang terjadi. Selain itu, masyarakat juga dianjurkan supaya berhati-hati dalam melakukan transaksi elektronik dan melindungi data pribadi mereka agar tidak menjadi korban kejahatan siber.

Keberhasilan dalam menangani kasus carding sangat bergantung pada ketepatan dan ketelitian dalam mengumpulkan serta menganalisis alat bukti elektronik. Pengumpulan alat bukti elektronik mencakup berbagai tahapan penting, mulai dari identifikasi sumber bukti, pemeliharaan integritas data, hingga pengujian forensik yang menyeluruh. Pertama, identifikasi sumber bukti melibatkan penentuan perangkat atau sistem yang digunakan dalam aktivitas carding, seperti komputer, ponsel, atau server. Penegak hukum harus memastikan bahwa semua perangkat yang relevan diidentifikasi dan diamankan dengan cepat untuk mencegah hilangnya data penting.

Selain pada hal tersebut, Analisis forensik juga memainkan peran vital dalam membongkar kasus carding. Proses ini melibatkan pemeriksaan mendetail terhadap data yang diperoleh untuk mengungkap pola, transaksi, atau komunikasi yang dapat mengindikasikan aktivitas ilegal. Para ahli forensik digital memakai beragam alat dan teknik canggih untuk memulihkan data yang terhapus, mengidentifikasi alamat IP yang digunakan, dan menganalisis log transaksi. Analisis ini sering kali perlu dilakukan dengan kehati-hatian dan mendalam untuk mengungkap jaringan pelaku yang mungkin tersebar di berbagai lokasi.

METODE PENELITIAN

Metode yang diterapkan dalam penelitian studi kasus ini adalah pendekatan yuridis normatif yang mengadopsi metode kualitatif. Dalam kerangka pendekatan yuridis normatif, penelitian ini mengandalkan analisis mendalam terhadap teori-teori hukum, konsep-konsep yang relevan, prinsip-prinsip hukum, dan kerangka peraturan perundang-undangan yang berlaku dalam konteks yang relevan dengan objek penelitian. Pendekatan ini bertujuan untuk memahami secara komprehensif bagaimana undang-undang diterapkan dan diinterpretasikan dalam situasi praktis, dengan mempertimbangkan dinamika dan kompleksitas aspek sosial-politik yang melingkupinya.

Penelitian ini secara spesifik memusatkan perhatian pada analisis penerapan undang-undang dalam konteks kasus carding di wilayah Bali. Untuk mencapai tujuan tersebut, penelitian merujuk pada dua kerangka hukum utama, yakni Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), yang relevan dengan substansi kasus yang sedang diteliti.

Metode kualitatif digunakan sebagai alat untuk menggali dan menganalisis secara rinci makna-makna yang terkandung dalam norma-norma hukum yang relevan dengan kasus tersebut. Pendekatan kualitatif memungkinkan peneliti untuk menjelajahi secara mendalam pemahaman tentang bagaimana norma-norma tersebut diinterpretasikan dan diterapkan dalam konteks kasus yang konkrit, serta memungkinkan untuk mengidentifikasi faktor-faktor kontekstual yang mempengaruhi proses tersebut. Dengan demikian, melalui pendekatan ini, diharapkan akan tercipta pemahaman yang lebih komprehensif dan kontekstual tentang implikasi hukum dari kasus carding di Bali.

HASIL DAN PEMBAHASAN

1. Elektronik Sebagai Alat Bukti Dalam Cybercrime

Sebuah bukti dianggap sah bukan hanya karena keberadaannya diatur dalam undang-undang (bewijsmiddelen), tetapi juga karena proses perolehan dan penyajian bukti tersebut di hadapan pengadilan (bewijsvoering). Selain itu, nilai kekuatan bukti (bewijskracht) yang dipersembahkan juga sangat memengaruhi penilaian hakim terhadap validitasnya.

Proses pembuktian dalam kasus cybercrime pada dasarnya menyerupai proses pembuktian dalam kasus pidana konvensional. Akan tetapi, dalam konteks kasus

cybercrime, unsur-unsur elektronik menjadi sangat signifikan, seperti kehadiran informasi atau dokumen elektronik. Regulasi hukum terkait proses pembuktian dalam kasus cybercrime telah dijelaskan dalam Pasal 5 ayat (1) dan ayat (2) Undang-Undang Nomor 19 Tahun 2016. Ketentuan tersebut menyatakan bahwa informasi dan/atau dokumen elektronik diakui sebagai alat bukti yang sah dalam proses pembuktian kasus cybercrime. Alat bukti elektronik ini dianggap sebagai perluasan dari alat bukti yang berlaku dalam hukum acara pidana di Indonesia, sejalan dengan alat-alat bukti yang diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Pasal 5 ayat (1) dari Undang-Undang Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016 menegaskan bahwa informasi elektronik dan/atau dokumen elektronik, termasuk hasil cetaknya, memiliki keabsahan sebagai alat bukti hukum. Hal ini mengindikasikan bahwa data yang disimpan, diproses, dan ditransmisikan secara elektronik memiliki status yang setara dengan bukti-bukti konvensional seperti kesaksian, surat, dan barang bukti fisik dalam konteks penerimaan bukti di pengadilan.

Pasal 5 ayat (2) menegaskan bahwa alat bukti elektronik dianggap sebagai perluasan dari jenis-jenis alat bukti yang sah sebagaimana yang disebutkan dalam Pasal 184 KUHAP (Kitab Undang-Undang Hukum Acara Pidana). Pasal 184 KUHAP secara khusus merinci jenis-jenis alat bukti yang dapat diterima secara legal, termasuk keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Oleh karena itu, dokumen elektronik dan informasi elektronik secara tegas diakui sebagai bagian dari kategori alat bukti yang sah, memberikan dasar hukum yang kuat untuk penggunaannya dalam proses peradilan pidana.

Agar suatu alat bukti elektronik dianggap sah dan memiliki kekuatan pembuktian yang kuat di pengadilan, maka cara memperoleh, menyimpan, dan mengelola informasi elektronik tersebut harus memenuhi ketentuan yang berlaku. Alat bukti elektronik harus didapatkan dengan cara yang legal dan sesuai prosedur, tidak boleh melalui tindakan yang melanggar hukum seperti hacking atau pengintaian ilegal.

2. Carding

Kejahatan carding adalah tindakan penipuan kartu kredit yang dilakukan oleh pelaku yang disebut carder, melalui berbagai cara, seperti membobol dan meretas kartu kredit via internet. Tujuannya adalah untuk memesan barang secara online atau mengambil dana secara ilegal dari rekening bank milik korban. Kejahatan carding ini memiliki beberapa bentuk, termasuk akses komputer secara ilegal (cyber trespass), pencurian informasi yang bernilai (cyber theft), penipuan melalui internet (cyber fraud), dan perusakan data (destructive cybercrimes).

Kejahatan di dunia maya, terutama dalam bentuk carding, dapat dijelaskan sebagai tindakan ilegal yang terjadi melalui jaringan internet, dimana pelaku memanfaatkan teknologi komputer dan telekomunikasi yang canggih. Pentingnya penanganan kejahatan ini tidak bisa diremehkan mengingat tingkat kompleksitasnya yang terus meningkat. Aktivitas kriminal dalam ranah cybercrime melibatkan penggunaan komputer atau jaringan komputer secara tidak sah dan melanggar hukum, yang bisa mencakup modifikasi atau penghancuran infrastruktur komputer yang diakses, yang pada gilirannya dapat mengakibatkan kerugian bagi pihak lain. Oleh karena itu, diperlukan peraturan khusus yang mengatur penanganan cybercrime, terutama dalam hal carding, sebuah kejahatan yang dianggap sebagai bagian dari kejahatan dunia maya yang menggunakan media internet dan teknologi elektronik.

Beberapa ketentuan hukum positif di Indonesia yang dapat menjadikan kejahatan carding sebagai tindakan kriminal terdapat dalam Pasal 362, Pasal 363 ayat (1), dan Pasal

378 KUHP. Pasal 362 KUHP mengatur tentang pencurian, dan dalam konteks kejahatan carding, pasal ini berlaku ketika pelaku mencuri informasi kartu kredit seseorang secara non fisik dengan menggunakan perangkat lunak. Pasal 363 ayat (1) KUHP, yang memuat unsur persengkongkolan, dapat diterapkan jika kejahatan carding dilakukan oleh pelaku yang bekerja sama dengan satu atau lebih orang lainnya. Sementara itu, Pasal 378 KUHP menyatakan bahwa tindakan penipuan untuk keuntungan pribadi atau orang lain adalah kriminal. Dalam kejahatan carding, pasal ini relevan jika pelaku menipu dengan menawarkan barang melalui iklan di website atau media sosial untuk memperoleh nomor kartu kredit korban dan menggunakannya untuk kepentingan pribadi. Jika modus operandi pelaku sesuai dengan penjelasan tersebut atau serupa, maka pasal ini dapat dikenakan pada pelaku kejahatan carding.

Selain pengaturan dalam KUHP, kejahatan carding juga diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Tahun 2016. UU ITE ini memberikan landasan hukum yang lebih spesifik untuk menangani kejahatan siber, termasuk carding. Beberapa pasal dalam UU ITE yang relevan untuk mengkriminalisasi kejahatan carding antara lain adalah Pasal 30, Pasal 31, Pasal 32, dan Pasal 36.

Dalam pasal 30 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik mengatur mengenai akses ilegal terhadap sistem komputer atau elektronik milik orang lain. Dalam konteks carding, pelaku seringkali mengakses sistem perbankan atau situs e-commerce tanpa izin untuk mencuri data kartu kredit. Pasal 30 ayat (1) menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain, dengan cara apapun, termasuk carding, dapat dikenakan hukuman pidana.

Selanjutnya dalam pasal 31 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik mengatur mengenai intersepsi atau penyadapan informasi elektronik. Pelaku carding dapat menggunakan teknik intersepsi untuk mencuri informasi sensitif, seperti nomor kartu kredit dan data pribadi lainnya, saat data tersebut sedang ditransmisikan. Misalnya, pelaku dapat memanfaatkan malware untuk mengakses informasi yang ditransmisikan dari komputer korban ke situs e-commerce.

Pada pasal 36 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan yang mengakibatkan kerugian bagi orang lain dalam melakukan transaksi elektronik, dapat dikenakan hukuman pidana. Dalam hal carding, pelaku yang menggunakan kartu kredit curian untuk berbelanja atau melakukan transaksi ilegal dapat merugikan pemilik kartu kredit secara finansial.

Tindakan pencegahan dalam menjaga keamanan dari penipuan carding melalui email dan situs web palsu sangatlah penting. Langkah yang paling dasar dan diperlukan adalah melakukan verifikasi yang cermat terhadap nama situs yang akan diakses. Apabila menerima email yang diduga berasal dari lembaga keuangan, sebaiknya segera melakukan pengecekan keaslian email tersebut dengan menghubungi langsung pihak terkait, seperti bank, untuk memastikan apakah email tersebut memang berasal dari lembaga tersebut atau tidak.

3. Kasus Tindak Pidana Carding Oleh Inisial MA

Seorang pria yang bernama M Arya Perdana Kusuma, berusia 41 tahun, dan berasal dari Jakarta Selatan, Provinsi DKI Jakarta, diidentifikasi sebagai pelaku carding oleh Kepolisian Daerah Bali. Tersangka ditangkap pada hari Selasa, tanggal 12 Juli 2023, saat berada bersama pasangannya di Mall Bali Galeria. Hasil penyelidikan menunjukkan bahwa pelaku merupakan ekse atau pengguna data kartu kredit (CC) yang dibeli dari Dark Web.

1. Pengungkapan pertama pada kasus Carding

   Kepala Bidang Hubungan Masyarakat Kepolisian Daerah Bali, Kombes Pol Jansen Avitus Panjaitan, menjelaskan bahwa penemuan ini bermula dari kegiatan patroli siber yang dilakukan oleh Direktorat Reserse Kriminal Khusus Kepolisian Daerah Bali pada tanggal 11 Juli 2023. Mereka menemukan adanya akun media sosial Instagram yang menggunakan nama "Ratdiba" yang mempromosikan pemesanan hotel atau vila dengan penawaran diskon sebesar 30-50 persen di AlI Hotel & Villa. Langkah selanjutnya melibatkan proses profilisasi terhadap akun media sosial tersebut, yang diduga dimiliki oleh RN. Dari situ, penyelidikan lebih lanjut dilakukan, dan RN diduga ditemukan di Mall Bali Galeria.
2. Penangkapan tersangka

   Pada hari Selasa, 12 Juli 2023, RN ditangkap di Mall Bali Galeria setelah diminta oleh pasangannya, yang juga menjadi tersangka, untuk memasang iklan pemesanan hotel atau vila. Mereka telah menjalin hubungan selama 2 bulan. RN tidak mengetahui asal usul voucher hotel tersebut, tetapi menurut pengakuan tersangka, voucher tersebut didapat dari promosi yang ditawarkan oleh berbagai agen perjalanan. Ketika petugas melakukan pemeriksaan terhadap laptop Macbook milik tersangka, ditemukan 1.293 data kartu kredit milik orang lain dari berbagai bank, baik domestik maupun internasional. Tersangka diduga sebagai ekse atau pengguna data kartu kredit (CC) orang lain yang dibeli di Dark Web. Data tersebut kemudian digunakan untuk memesan atau membeli voucher hotel atau tiket pesawat melalui aplikasi Airbnb atau Booking.com, serta aplikasi di App Store Apple.
3. Pengungkapan Alat Bukti Elektronik

   Dalam kasus carding ini, tersangka diduga telah memanfaatkan akun milik individu lain untuk mempromosikan penjualan tiket dan layanan hotel tanpa izin yang sah. Sementara itu, barang bukti yang berhasil disita oleh pihak berwenang meliputi sejumlah aset digital dan materi fisik yang menjadi bukti pendukung dalam penyelidikan. Di antaranya adalah sebuah laptop merk Apple Macbook Pro dengan warna Space Grey, dua unit ponsel iPhone, dua akun yang terkait dengan aktivitas di Dark Web, sebuah kendaraan bermotor tipe Mini Cooper, aplikasi perbankan BCA Mobile, serta aplikasi Blu By BCA.
4. Dasar Hukum yang Digunakan

   Dalam kasus carding di Bali, terdakwa yang disebut sebagai MA didakwa melanggar Pasal 32 ayat (1) yang berkaitan dengan transmisi, modifikasi, penambahan, dan tindakan terkait informasi elektronik tanpa izin yang diatur dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ancaman hukuman yang dihadapi terdakwa mencakup penjara maksimal selama 8 tahun serta denda sebesar Rp 2 miliar.

   Pasal 32 ayat (1) dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menegaskan bahwa setiap individu harus memperoleh izin terlebih dahulu sebelum melakukan serangkaian tindakan terhadap informasi elektronik yang dimiliki oleh orang lain. Dalam konteks ini, MA dituduh melakukan tindakan carding yang melibatkan penggunaan kartu kredit tanpa izin dari pemiliknya.

   Selanjutnya, Pasal 48 ayat (1) dari Undang-Undang yang sama menetapkan hukuman maksimal bagi pelaku tindakan sebagaimana diatur dalam Pasal 32 ayat (1), yakni hukuman penjara maksimal 8 tahun dan denda hingga Rp 2 miliar. Akibatnya, MA menghadapi risiko hukuman yang serius dan berat atas tindakannya.

5. Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Carding

Sebelum adanya Undang-Undang tentang Informasi dan Transaksi Elektronik disahkan, contohnya tantangan dalam menangani kejahatan siber adalah bahwa bukti seperti perangkat lunak, data elektronik, atau bukti elektronik lainnya belum diakui sebagai alat bukti yang sah dalam hukum Indonesia.

Pasal 28 Ayat (1) dalam Undang-Undang Republik Indonesia Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman menegaskan bahwa hakim memiliki kewajiban untuk memiliki pemahaman yang mendalam terhadap nilai-nilai hukum dan keadilan yang berlaku dalam masyarakat. Dengan demikian, sangatlah penting bagi hakim untuk mengakui dan memahami peran serta signifikansi dari alat bukti elektronik dalam menangani kasus-kasus kejahatan siber dan transaksi elektronik. Sebagai upaya untuk memberikan kejelasan hukum, regulasi terkait dengan penggunaan alat bukti elektronik seharusnya diatur secara tegas dalam undang-undang, seperti yang telah dilakukan melalui Undang-Undang tentang Informasi dan Transaksi Elektronik (ITE).

Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diamandemen dengan Undang-Undang Nomor 19 Tahun 2016, bukti elektronik diakui sebagai bukti yang sah menurut hukum apabila memenuhi kriteria berikut ini:

a. Keaslian: Bukti elektronik haruslah asli dan tidak mengalami manipulasi.
b. Keterkaitan: Bukti elektronik harus relevan dengan tindak pidana yang dituduhkan.
c. Kemampuan Pembuktian: Bukti elektronik harus memiliki kemampuan untuk membuktikan tindak pidana yang dituduhkan.

Pasal 183 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang membahas persyaratan formil dan materil terkait dengan alat bukti elektronik, juga mengamanatkan bahwa persyaratan yang sama harus dipenuhi diantara lain:

a. Syarat formil
   bukti elektronik harus sah yaitu otentik (diambil dari pemilik yang sah) dan terjaga integritasnya.
b. Syarat materil
   bukti elektronik harus relevan atau sesuai dengan tindak pidana dan identitas terdakwa.

Pembuktian terhadap alat bukti berupa data elektronik juga melibatkan evaluasi terhadap validitasnya, karena karakteristik khusus dari bukti elektronik yang tercatat dalam perangkat elektronik, membuatnya rentan terhadap rekayasa dan keraguan akan keabsahan informasinya. Selain itu, dalam proses pembuktian, perlu dilakukan analisis mendalam terhadap integritas dan otentisitas data elektronik tersebut untuk memastikan keabsahannya sebagai bukti yang sah dalam pengadilan

Hal ini melibatkan langkah-langkah teknis seperti verifikasi sumber data, pencatatan jejak digital yang ketat, serta penilaian terhadap proses pengumpulan, penyimpanan, dan pengolahan informasi elektronik secara keseluruhan. Dengan demikian, penggunaan bukti elektronik dalam ranah hukum menuntut pemahaman yang mendalam tentang teknologi informasi dan keahlian khusus dalam melakukan audit digital untuk menjamin keandalan dan keabsahan bukti yang disajikan di pengadilan.

Dalam kajian kasus carding ini, alat bukti elektronik memainkan peran penting dalam beberapa aspek kunci:

1. Mengidentifikasi Pelaku

Pada intinya, carding, merupakan tindakan kriminal di mana pelaku mencuri data

elektronik dari kartu kredit korban. Data tersebut kemudian disalin ke kartu kredit baru, yang kemudian digunakan untuk menarik uang tunai atau melakukan pembelian untuk keuntungan pelaku. Semua tagihan dari aktivitas ini dibebankan kepada korban.

Pada kasus yang dikaji, data kartu kredit yang ditemukan di laptop Macbook milik MA dapat digunakan untuk mengidentifikasi pemilik kartu kredit yang sah. Informasi ini memungkinkan penyidik untuk melacak jejak pembelian tiket yang dilakukan menggunakan kartu kredit tersebut, sehingga dapat menghubungkan tindakan ilegal dengan MA.

2. Membuktikan Tindak Pidana Carding

   Data kartu kredit yang telah digunakan untuk membeli tiket dengan harga murah menjadi salah satu bukti penting. Bukti ini menunjukkan bahwa MA telah memanfaatkan informasi kartu kredit curian untuk keuntungan pribadi. Selain itu, bukti transaksi pembelian data kartu kredit di Dark Web menunjukkan bahwa MA terlibat dalam perdagangan ilegal informasi keuangan. Bukti-bukti ini bersama-sama memberikan dasar kuat bahwa MA telah melakukan tindak pidana carding, melanggar undang-undang terkait dengan penipuan dan pencurian data.

3. Melacak Jejak Digital

   Selain dari data kartu kredit, terdapat berbagai bentuk log aktivitas pada laptop, riwayat penelusuran di browser, serta komunikasi melalui email atau pesan instan yang bisa memberikan petunjuk berharga tambahan tentang metode dan jaringan kriminal yang dimanfaatkan oleh MA. Bukti-bukti elektronik ini memungkinkan penyelidik untuk membangun gambaran yang lebih lengkap dan rinci mengenai modus operandi yang digunakan oleh pelaku. Dengan menggabungkan informasi dari berbagai sumber digital, para penyidik dapat mengidentifikasi pola-pola tertentu, memahami struktur jaringan kejahatan, dan mengungkap lebih dalam tentang strategi yang diterapkan.

4. Menguji Keterlibatan Pelaku

   Bukti dari perangkat elektronik dapat menunjukkan keterlibatan langsung MA dalam kejahatan carding. Misalnya, rekaman video atau audio dari kamera atau mikrofon laptop, pesan-pesan chat yang mengindikasikan niat atau rencana untuk melakukan kejahatan, dan dokumen-dokumen digital terkait transaksi ilegal semua bisa digunakan untuk membuktikan keterlibatan MA di pengadilan.

   Tersangka dihadapkan pada dakwaan yang merujuk pada Pasal 32 ayat 1 yang terkait dengan Pasal 48 ayat 1 dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Jika terbukti bersalah, tersangka dapat dikenai sanksi pidana penjara dengan masa tahanan maksimal 8 tahun dan/atau denda sebesar Rp. 2 miliar.

   Dengan demikian, alat bukti elektronik tidak hanya membantu dalam mengidentifikasi pelaku tetapi juga memberikan dasar yang kuat untuk membuktikan bahwa tindak pidana carding telah dilakukan, serta menguraikan cara dan jaringan kerja pelaku dalam melakukan kejahatan tersebut.

   Di sisi lain, kasus kejahatan carding terus berlangsung dengan berbagai metode operasi yang berbeda. Penanganan kasus ini masih menghadapi sejumlah kendala, di antaranya adalah kurangnya kesadaran dari nasabah akan pentingnya menjaga keamanan data pribadi, contohnya identitas, nomor PIN, dan kode OTP. Persoalan ini semakin berkembang seiring berjalannya waktu, mengancam baik nasabah maupun lembaga perbankan.

SIMPULAN

Berdasarkan kasus carding di Bali pada tahun 2023 yang melibatkan MA sebagai pelaku carding, dapat disimpulkan bahwa alat bukti elektronik memainkan peran kunci dalam mengungkap dan membuktikan tindak pidana carding. Data elektronik dari laptop pelaku, Penggunaan data kartu kredit milik orang lain untuk transaksi ilegal, yang dijadikan sebagai bukti dalam proses peradilan pidana, diatur sebagai bagian yang sah. Regulasi hukum terkait cybercrime, seperti Undang-Undang Informasi dan Transaksi Elektronik, juga memiliki peran penting dalam menangani kasus semacam ini.

Alat bukti elektronik diakui sebagai bukti yang valid saat proses peradilan pidana, termasuk pada kasus carding di Bali. Kejahatan carding, yang merupakan tindakan penipuan kartu kredit yang dilakukan secara online, menjadi sorotan dalam kasus ini. Pelaku carding di Bali menggunakan kartu kredit orang lain untuk memesan tiket pesawat dan hotel, yang kemudian dijerat dengan Undang-Undang Informasi dan Transaksi Elektronik dan diancam hukuman penjara maksimal 8 tahun dan denda Rp 2 miliar. Pentingnya keaslian, keterkaitan dengan tindak pidana, dan integritas data elektronik dalam proses pembuktian menjadi faktor kunci untuk memastikan keabsahan bukti di pengadilan.

Data kartu kredit yang digunakan untuk membeli tiket dengan harga murah dalam kasus carding di Bali menjadi bukti tindak pidana yang kuat. Bukti elektronik dari laptop pelaku dan aktivitas online juga turut membantu mengidentifikasi pelaku dan memperkuat kasus di pengadilan. Dengan adanya Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, pelaku carding dihukum sesuai dengan peraturan yang berlaku, menegaskan pentingnya penegakan hukum yang efektif dalam menangani kejahatan cyber seperti carding.

Disarankan agar penegak hukum terus meningkatkan keahlian dalam melakukan audit digital, memperkuat kerjasama antar lembaga terkait seperti Kementerian Komunikasi dan Informatika dan kepolisian. Serta Badan Siber dan Sandi Negara (BSSN), serta mengedukasi masyarakat tentang pentingnya melindungi data pribadi pada transaksi elektronik guna mencegah menjadi korban kejahatan siber. Dengan langkah-langkah proaktif ini, diharapkan penegakan hukum terhadap kejahatan cyber seperti carding dapat menjadi lebih efisien dan efektif. Serta untuk mempercepat digitalisasi dan menghadapi serangan kejahatan siber, pemerintah memerlukan bantuan seluruh masyarakat. Setiap individu dapat berperan aktif dengan cara menanggapi informasi dengan benar, meningkatkan kesadaran pentingnya keamanan informasi, mengembangkan sumber daya manusia, dan menggunakan teknologi informasi secara bijaksana.

DAFTAR PUSTAKA

Artikel

Santoso, S. (2018). Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional. Jurnal Lemhannas RI, 6(2), 43-48.

Malalangi, H. E. (2022). Pertanggung Jawaban Pidana Pelaku Pembobolan Kartu Kredit Dengan Modus Carding Menurut Undang-Undang Informasi Dan Transaksi Elektronik. Lex Crimen, 11(3).

Ginara, I. G. K., Widyantara, I. M. M., & Styawati, N. K. A. (2022). Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime dalam Hukum Pidana Indonesia. Jurnal Preferensi Hukum, 3(1), 138-142.

Siregar, V. A. (2021). Fenomena Kejahatan Carding Berdasarkan dalam Hukum Pidana Indonesia. Jurnal Hukum Das Sollen, 6(2), 99-124.

Lasmadi, S. (2014). Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya. Jurnal Ilmu Hukum Jambi, 5(2), 43274.

Putra, B. A. D., & Wahjuningati, E. (2022). Kedudukan Alat Bukti Elektronik Yang Diperoleh Dari Penyadapan Hacker Dalam Hukum Pidana. Judiciary (Jurnal Hukum Dan Keadilan).

Pujoyono, N. W. (2020). Penal Policy dalam Upaya Preventif Kejahatan Carding di Indonesia. Jurnal Panji Keadilan: Jurnal Ilmiah Nasional Mahasiswa Hukum, 3(1), 86-98.

Kurniawan, AB, & Soeskandhi, H. (2022). Perlindungan Hukum Terhadap Pengguna Electronic Banking Atas Tindak Pidana Carding Dilihat Dari Hukum Informasi Dan Transaksi Elektronik. SUPREMISASI: Jurnal Hukum , 5 (1), 64-87.

Kartika, PP (2019). Data Elektronik Sebagai Alat Bukti Yang Sah Dalam Pembuktian Tindak Pidana Pencucian Uang. Jurnal Hukum Pidana Indonesia , 1 (1), 33-46.

Firmansyah, N. M. I., & Nurfanto, L. (2021). Pertanggungjawaban Pidana Carding Terhadap Pengguna Kartu Kredit. Mimbar Hukum, 14(2), 206-217.

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. Justisia: Jurnal Ilmu Hukum, 1(1), 1-11.

Buku

Ali, Z. (2021). Metode penelitian hukum. Sinar Grafika.

Undang-Undang

Undang-undang (UU) No. 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Artikel Berita

Ayu Afria Ulita Ermali, (2023, Juli 28), “Polda Bali Ungkap Kasus Carding, Pelaku Diamankan di Mall” (https://bali.idntimes.com/news/bali/ayu-afria-ulita-ermalia/polda-bali-ungkap-kasus-carding-2?page=all&_gl=1*1g40wgl*_ga*TXU2ZUVzRk1idVZBLTRxeUVJRDJZZ3B6dVVELTVidFFvNnN6WDNOZk0xMWNjX2JmMUtGM1UwNHhGMUktYm00dw..*_ga_TT180KERFB*MTcxNjUzOTkyOS4xLjAuMTcxNjUzOTkyOS4wLjAuMA) diakses pada 24 Mei 2024.

Rolandus Nampu (2023, Juli 28), “Polda Bali tangkap pelaku kejahatan pencurian 1.293 data kartu kredit” https://m.antaranews.com/amp/berita/3656613/polda-bali-tangkap-pelaku-kejahatan-pencurian-1293-data-kartu-kredit diakses pada 23 mei 2024