# KAJIAN NORMATIF PENANGANAN *CYBER CRIME* DI SEKTOR PERBANKAN DI INDONESIA

Abdurrakhman Alhakim[1], Sofia[2]

Fakultas Hukum, Universitas Internasional Batam, Indonesia

e-mail: alhakim@uib.ac.id, szhen45@gmail.com

**ABSTRAK**

Sebagai tempat perputaran uang, bank memiliki kedudukan yang rentan terhadap penyalahgunaan kewenangan, baik oleh pihak bank sendiri maupun oleh pihak luar yang memanfaatkan bank sebagai tempat untuk menyembunyikan hasil kejahatannya. Akan tetapi terdapat kegiatan perbankan memiliki motif tertentu sehingga melampaui atau tidak sesuai dengan ketentuan yang berlaku. Kegiatan semacam ini disebut kejahatan perbankan atau tindak pidana perbankan. Mengingat *Cyber Crime* menggunakan teknologi yang tinggi sebagai media, maka kebijakan kriminalisasi di bidang teknologi informasi juga harus memperhatikan perkembangan upaya penanggulangan *Cyber Crime* di Indonesia. Metode Pendekatan yang digunakan dalam penelitian ini adalah metode yuridis empiris. Jenis data yang dipakai merupakan data primer yang didapatkan melalui penelitian lapangan yang diperoleh dari hasil observasi lapangan berhubungan dengan penanganan *Cyber Crime* terhadap sektor perbankan. Pencegahan dan penanggulangan kejahatan perbankan tak dapat diserahkan hanya kepada salah satu pihak saja dalam penegakan hukum, sehingga bukan hanya penyebab kausatif atau simptomatik yang terselesaikan, akan tetapi penyebab yang bersifat komprehensif dan dapat di atasi secara bersama-sama.

**Kata kunci:** *cybercrime*, perbankan, kejahatan.

***ABSTRACT***

*As a place for money circulation, banks have a position that is vulnerable to abuse of authority, both by the bank itself and by outside parties who use the bank as a place to hide the proceeds of their crimes. However, there are banking activities that have certain motives so that they exceed or do not comply with applicable regulations. Such activities are called banking crimes or banking crimes. Considering that Cyber Crime uses high technology as a medium, the criminalization policy in the field of information technology must also pay attention to the development of Cyber Crime prevention efforts in Indonesia. Method The approach used in this research is the empirical juridical method. The type of data used is primary data obtained through field research obtained from field observations related to the handling of Cyber Crime against the banking sector. Prevention and control of banking crimes cannot be left to only one party in law enforcement, so that not only causative or symptomatic causes are resolved, but causes that are comprehensive and can be overcome together.*

**Keywords:** *cybercrime*, banking, crime.

## PENDAHULUAN

Sebagai tempat tukar menukar uang, bank memiliki posisi yang berbahaya terhadap penyalahgunaan uang itu sendiri, baik oleh pihak bank ataupun dari pihak luar yang memanfaatkan bank sebagai tempat dalam menyembunyikan hasil kejahatannya (Disemadi & Shaleh, 2020; Shahrullah, 2014), akan tetapi ditemukan aktivitas perbankan yang memiliki keinginan tertentu sehingga melewati atau tidak sesuai dengan ketentuan yang resmi (Disemadi & Prananingtyas, 2019; Disemadi, 2019). Kegiatan semacam ini dinamakan kejahatan perbankan ataupun tindak pidana perbankan. Tindak pidana perbankan yang mampu dilakukan untuk berbagai aktivitas perbankan tersebut berkaitan melalui sistem keamanan ketika menjalankan tiap kegiatannya (Arofah & Priatnasari, 2020). Sistem keamanan tidak hanya menyangkut SDM saja, namun juga sarana serta prasarana yang hingga saat ini terus berkembang (Sulisrudatin, 2018) Oleh sebab itu, sesudah komputer terkenal di berbagai belahan dunia, maka orangpun lalu disibukkan serta direpotkan pula dengan efek samping yang muncul, yakni berupa kejahatan komputer (*cyber crime*) (Anin, 2020).

TB. Ronny R. Nitibaskara menyebutkan *cyber crime* sebagai kejahatan yang terjadi berkaitan ataupun terhadap jaringan komputer di dalam internet (Widodo, 2009). Namun pada umumnya, istilah *cyber crime* merujuk terhadap suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) serta perilaku yang memakai komputer (Mansur & Gultom, 2009). Secara harfiah *cybercrime* merupakan penyebutan yang mengaitkan terhadap kegiatan kejahatan melalui komputer maupun jaringan komputer menjadi sarana, sasaran ataupun lokasi terjadinya kejahatan. Termasuk didalamnya antara lain yaitu penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit (*carding*), *confidence fraud,* penipuan identitas, pornografi anak, dan lain-lain. Polri mengeluarkan kerugian dari kegiatan kejahatan perbankan yang mensasar sistem pembayaran di Indonesia. Kerugian mencapai hingga angka Rp. 33 miliar selama periode 2012-2015. "Periode 2012-2015 akumulasi Rp 33 miliar, pelakunya 497 orang," menurut Direktur Tindak Pidana Ekonomi dan Khusus Bareskrim Mabes Polri (Dirtipideksus) Bareskrim Polri, Brigjen Victor Simanjuntak ketika acara seminar pencegahan kejahatan dunia maya di BI, Jakarta, Selasa (28/4/2015) (Sutianto, 2015). Melalui data selama dua tahun terakhir, Subdirektorat *Cyber Crime* Bareskrim Polri telah mendapatkan 101 laporan pencurian uang nasabah oleh 35 negara dengan total kerugian hingga puluhan miliar rupiah (Sutianto, 2015).

Modus operasi yang dilaporkan pun beraneka-ragam, mulai dari penipuan penjualan barang, penipuan melalui pemalsuan alamat email, penipuan lewat penanaman saham, membajak ATM nasabah sampai memalsukan mesin ATM supaya mampu dibobol (Kuwado, 2015). Akan tetapi, kejahatan jenis tersebut kerap tak terdeteksi dan bahkan dalam banyak hal aparat penegak hukum justru kalah terampil dari pelakunya, baik itu yang berkenaan dengan objek yang menjadi sasaran kejahatan maupun masalah pembuktian dalam proses peradilan. Contoh *cybercrime* dalam transaksi perbankan yang memakai sarana internet sebagai basis transaksi yakni sistem layanan kartu kredit serta layanan perbankan online (*online banking)* (Ratulangi, 2021).

Peringkat pembobolan kartu kredit di Indonesia masih berada di posisi kedua terendah jika disandingkan dengan negara lain di wilayah Asia Pasifik. Sedangkan melalui data Visa, peringkat *fraud* Indonesia berada di posisi ketiga terendah dibandingkan dengan negara lain di Asia Tenggara. Data terakhir Bank Indonesia (BI) sebagai otoritas moneter mencatat, pada bulan Mei 2013, telah ditemukan hingga 1.009 kasus pembobolan (*fraud*) yang dilaporkan dengan nilai kerugian sampai Rp 2,37 miliar. Kejahatan kartu kredit yang paling banyak terjadi yakni pencurian indentitas serta *Card Not Present* (CNP). Malalui jumlah kasus pencurian identitas sejumlah 402 kasus dan CNP 458 kasus dengan nilai masing masing Rp 1,14 miliar serta Rp 545 juta yang dirasakan 18 penerbit (Sari, 2015). Salah satu kasus pencurian data kartu kredit yang sukses diungkap dari pihak kepolisian yakni ditemukannya penjahat penipu *credit card*, berinisial BA (37) serta AL (37). Direktur Kriminal Umum Polda Metro Jaya Kombes Pol Khrisna Murti menyebutkan, kedua pelaku sukses mengambil uang melalui bank swasta melalui kartu kredit korban sejumlah ratusan juta rupiah (Novita, n.d).

Modus operasi kedua pelaku, yakni melalui pembelian daftar nasabah yang berisi data pemilik kartu kredit salah satu bank swasta melalui pihak marketing. Mereka beralasan menawarkan asuransi jiwa, yang dikerjakan pelaku BA. Setelah sukses memperoleh daftar informasi pribadi pemegang kartu kredit, tersangka BA menghubungi nomor telepon pemilik kartu kredit yang berada di dalam data tersebut lalu mengaku dari *credit card* pusat bank swasta. Selanjutnya terhadap seluruh korban, BA menjelaskan lalu menggunting kartu kredit korban malelui modus akan menggantinya dengan kartu kredit baru ditambah limit yang lebih besar tanpa harus membayar administrasi. Lalu salah satu pelaku, yaitu AL bertugas sebagai kurir dalam mengambil kartu kredit korban berikut fotokopi KTP melalui alasan agar menyesuaikan informasi serta memberi tanda terima dengan logo salah satu bank dengan nama pemilik kartu kredit. Pelaku BA membuat KTP palsu dengan data identitas fotokopi KTP korban yang akan dipakai sewaktu mengerjakan transaksi di toko agar

membeli barang-barang mewah (Andini, 2015).

Kejahatan perbankan berkaitan *cybercrime* salah satunya merupakan pencurian data kartu kredit (*fraud*). Motif kejahatan tersebut dinilai karena munculnya faktor pekerjaan serta munculnya peluang ataupun kesempatan dalam menipu daya korban sampai memilih memberikan kartu kredit kepada pelaku. Di dunia perbankan, evolusi *Cyber Crime* cukup mengejutkan khususnya disebabkan adanya sejumlah kasus yang merugikan pihak perbankan contohnya kasus pembobolan melalui *e-banking* yang terjadi terhadap sejumlah bank besar di Indonesia seperti bank *Bank Central Asia* (BCA) serta Bank Mandiri (Soetarto, 2015). Sementara itu beberapa pengguna maupun pemilik *credit card* juga kecewa, disebabkan nomor kartu kreditnya sudah dipakai pihak lain dalam melakukan transaksi *e-commerce* sampai menimbulkan kerugian yang amat besar. Hal tersebut wajib memperoleh perhatian mengingat karakteristik *Cyber Crime* sangat berbeda dengan tindak pidana konvensioal serta karakteristiknya yang bersifat *borderless* membuat pendekatan hukum di bidang tersebut tidak bisa lagi dikerjakan melalui cara konvensional. Selain itu, *Cyber Crime* memakai teknologi yang tinggi sebagai alat untuk kejahatan, sehingga kebijakan kriminalisasi di bidang teknologi informasi juga wajib melihat evolusi usaha dalam menanggulangi *Cyber Crime* di Indonesia, khususnya di bidang perbankan.

## METODE

Metode Pendekatan yang digunakan dalam penelitian ini merupakan metode yuridis empiris. Jenis data yang dipakai merupakan data primer yang didapatkan melalui penelitian lapangan yang diperoleh dari hasil observasi lapangan berhubungan dengan penanganan *Cyber Crime* terhadap sektor perbankan yang terdiri melalui sejumlah bahan hukum primer yang berupa peraturan perundang-undangan yang resmi, bahan hukum sekunder memberikan penjelasan tentang bahan hukum primer serta bahan hukum tersier yaitu memberikan petunjuk ataupun penjelasan terhadap bahan hukum primer dan sekunder. Metode Pengumpulan data yang digunakan terdiri dari 2 yaitu penelitian kepustakaan serta penelitian lapangan. Setelah semua data terkumpul lalu dikerjakan pemeriksaan terhadap data yang sudah ada. Data tersebut diolah dan disusun secara sistematis (Shahrullah, 2014)

## HASIL DAN PEMBAHASAN

### A. Penanganan Kasus *Cybercrime* di Indonesia Saat ini

Ketentuan hukum yang dapat dipakai agar menyeret pelaku *Cyber Crime* tersebut baru sebatas pada Peraturan perundang-undangan Kitab Undang-undang Hukum Pidana (KUHP) dan Undang-undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Ketentuan lainnya, jikapun ada, tersebar terhadap berbagai peraturan perundang-undangan serta tidaklah bersifat spesifik. Sedangkan Amerika telah mempunyai sejumlah Peraturan Perundang-undangan yang dengan tegas mengatur tentang *Cyber Crime* contohnya *Title 18 U.S. Code 1030* yang mengatur tentang *Fraud and related activity in connection with computers,* mengatur mengenai Bank *Fraud* dan *Title 18 U.S. Code 2252B* yang mengatur mengenai *Misleading domain names on the internet*. Selain itu Amerika juga merupakan anggota dari *Convention on Cyber Crime (Budapest Convention 2001*) merupakan organisasi yang berkeinginan melakukan perlindungan terhadap masyarakat dari kejahatan di dunia Internasional (Shahrullah, 2014). Organisasi tersebut mampu mendeteksi seluruh pelanggaran yang ada di seluruh dunia. Indonesia yang bukan merupakan anggota dari konvesi tersebut sangatlah dirugikan dikarenakan konvensi tersebut menghasilkan suatu peraturan perundang-undangan yang amat efektif sebagai bentuk pelindungan terhadap perilaku *Cyber Crime*. Sehingga dalam hal penanganan mengenai *Cyber Crime* jika dibandingkan dengan Amerika, Indonesia masih kurang efektif.

Hal ini dipengaruhi beberapa faktor antara lain dikarenakan peraturan perundang-undangan yang tidak mengatur secara rinci terhadap pelaku yang telah melanggar peraturan tersebut dan belum optimalnya pelaksanaan penanganan yang dilakukan oleh para penegak hukum. Polda Kepri khususnya pada Subdit Ditreskrimsus unit pelanggaran *cybercrime* yang telah didirikan pada bulan

Maret tahun 2014 lalu yang berwenang melakukan penanganan terhadap pelanggaran *cybercrime* menyatakan bahwa pelanggaran *cybercrime* merupakan jenis pelanggaran yang tidak mudah untuk ditangani, hal ini dikarenakan proses pencaharian pelaku dan barang bukti pelanggaran tidaklah mudah. Berdasarkan informasi yang diperoleh dari hasil wawancara kepada pihak kepolisian pada unit *cybercrime* ini jumlah pelanggaran *cybercrime* secara umum di seluruh Indonesia yang meliputi perbuatan penghinaan, penipuan, pelecehan yang dilakukan melalui media sosial, perjudian online berjumlah sekitar 400 kasus setiap tahunnya dan khususnya yang merugikan sektor perbankan di seluruh Indonesia berjumlah antara 103 sampai dengan 120 kasus per tahun dalam jangka waktu 5 tahun terkahir ini (Shahrullah, 2014). Dari jumlah pelanggaran tersebut diatas, kasus yang telah selesai ditangani oleh pihak kepolisian adalah sebanyak 45 sampai dengan 60 kasus yang telah diserahkan ke Kejaksaan untuk ditindak lanjuti, sedangkan sisanya masih berada dalam proses penanganan oleh pihak kepolisian. Menurut pihak kepolisian, kasus-kasus yang belum selesai tersebut sulit untuk ditangani dikarenakan mengalami kendala-kendala antara lain dalam mengumpulkan alat bukti pelanggaran yang karena sifat pelanggaran yang digital mengharuskan para penyidik juga memiliki alat dengan teknologi yang maju agar dapat menemukan alat bukti tersebut, tim penyidik yang masih kurang, proses penangkapan terhadap pelaku pelanggaran *cybercrime* yang berada diluar yurisdiksi negara Indonesia yang dikarenakan tidak adanya kerjasama negara Indonesia dengan negara-negara lainnya. Namun, berdasarkan informasi yang penulis peroleh, guna menangkap pelaku pelanggaran *cybercrime,* walau masih mengalami banyak kendala dan kesulitan.

Hal tersebut tidak membuat pihak kepolisian kehilangan akal dan cara, pihak kepolisian masih memiliki cara-cara lain yang dipergunakan untuk mencari alat bukti maupun pelaku yang berada diluar negeri. Bentuk tindakan yang telah dilakukan oleh pihak kepolisian antara lain menjalin hubungan dan bekerjasama dengan pihak kepolisian negara lain sehingga dapat membantu proses penangkapan pelaku *cybercrime* didaerah persembunyiannya. Kejahatan di bidang perbankan disebut juga kejahatan apapun yang berkaitan perbankan, contohnya seorang perampok bank merupakan kejahatan di bidang perbankan, begitu juga pengalihan rekening secara tidak sah merupakan kejahatan di bidang perbankan, jadi pengertiannya sangat luas. Sedangkan, kejahatan perbankan yaitu bentuk perbuatan yang telah diciptakan oleh undang-undang perbankan yang merupakan larangan serta keharusan, misalnya larangan mendirikan bank gelap serta membocorkan rahasia bank. Perbedaan isitlah tersebut memunculkan ataupun berpengaruh terhadap penindakan hukum. Kejahatan perbankan akan ditindak melalui ketentuan pidana yang diatur dalam undang-undang perbankan, sedangkan kejahatan di bidang perbankan ditindak melalui undang-undang di luar undang-undang perbankan (Yulia, 2010).

UU No. 10 Tahun 1998 tidak merumuskan pengertian tentang tindak pidana perbankan. UU tersebut hanya mengkategorikan beberapa perbuatan yang termasuk ke dalam kejahatan dan di satu pihak bisa dikategorikan sebagai suatu pelanggaran. Akan tetapi ada juga yang membedakan pengertian tindak pidana perbankan dengan tindak pidana di bidang perbankan.

Tindak pidana di bidang perbankan adalah segala jenis perbuatan melanggar hukum yang berhubungan dengan kegiatan dalam menjalankan usaha bank, baik bank sebagai sasaran maupun sebagai sarana, sedangkan tindak pidana perbankan (*banking crime*) merupakan tindak pidana yang dilakukan oleh bank (Yulia, 2010). Adapun karakteristik dalam tindak pidana perbankan adalah bank bisa sebagai korban maupun sebagai pelaku. Bank sebagai korban misalnya dalam hal penipuan, pemalsuan surat-surat bank, dan bank sebagai pelaku misalnya perbuatan *window dressing*, menetapkan suku bunga berlebihan, memberikan kartu kredit yang tidak wajar, menjalankan usaha bank dalam bank, menjalankan usaha bank tanpa ijin serta menjalankan usaha yang menyerupai bank. *Cybercrime* disebut juga sebagai salah satu bentuk ataupun dimensi baru dari kejahatan di zaman sekarang yang memperoleh perhatian khusus di dunia internasional (Arief, 2001).

Dalam arti sempit *cybercrime* merupakan *computer crime* yang bertujuan jahat terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, *cybercrime* berkaitan dengan seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunaanya ataupun jenis-jenis kejahatan tradisional yang sekarang dikerjakan melalui pemakaian maupun juga bantuan sarana komputer (*computer related crime*)(Akbar,2014). Dari pengartian tersebut, maka dalam arti sempit *cyber crime* merupakan *computer crime* yang bertujuan jahat terhadap sistem ataupun jaringan komputer, sedangkan dalam arti luas, *cybercrime* mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer serta pemakaiannya maupun jenis-jenis kejahatan tradisional yang sekarang dikerjakan melalui pemakaian maupun melalui bantuan sarana komputer (*computer related crime*). aktivitas yang berpotensi menjadi target *cybercrime* dalam aktivitas perbankan yang pertama yakni layanan pembayaran memakai kartu kredit di web toko online, kedua yaitu layanan perbankan online (*online banking*). Dapat diketahui terdapat sejumlah macam-macam dari *cybercrime* apabila dilihat melalui kegiatannya, yakni *Carding* yaitu berbelanja memakai nomor serta identitas kartu kredit orang lain, yang didapatkan secara ilegal, biasanya melalui pencurian informasi di internet. Sebutan pelakunya yakni *"carder"*. Sebutan lain dalam kejahatan macam ini yaitu *cyberfroud* atau istilahnya penipuan di dunia maya. Selanjutnya *Hacking* merupakan penerobosan program komputer milik orang ataupun sebuah instansi lain. *Hacker* disebut juga sebagai orang yang gemar membongkar komputer, memiliki keterampilan dalam membuat dan membaca program tertentu serta terobsesi mengamati keamanan (security)-nya. *Cracking* merupakan *hacking* dengan tujuan kejahatan. Sebutan sebagai *"cracker"* yakni *"hacker"* bertopi hitam *(black hat hacker)*. Berbeda dengan *"carder"* yang hanya mengintip kartu kredit, *"cracker"* mengintip simpanan para nasabah di berbagai bank ataupun pusat data sensitif lainnya sebagai keuntungan diri sendiri.

*Defacing* merupakan aktivitas mengganti halaman situs/website pihak lain, seperti yang terjadi terhadap situs Menkominfo, Partai Golkar, BI baru-baru ini serta situs KPU. *Phising* merupakan aktivitas memancing pengguna komputer di internet *(user)* supaya bersedia memberi informasi data diri pengguna *(username)* serta kata sandinya *(password)* terhadap suatu website yang sudah di-*deface*. *Spamming* merupakan pengiriman berita ataupun iklan melalui surat elektronik *(e-mail)* yang tak diinginkan oleh pengguna. *Malware* merupakan program komputer yang mencari kelemahan dari suatu software. biasanya *malware* dibuat supaya membobol ataupun merusak suatu software serta *operating system*. Modus operasi dalam hal bank sebagai korban tidak begitu banyak, biasanya hanya dalam bentuk pemalsuan dokumen, penggelapan dan korupsi, pelakunya biasanya orang, bukan korporasi. Apabila pelakunya adalah bank (sebagai korporasi), modus operasinya dapat bermacam-macam. Kejahatan tersebut dikelompokkan sebagai *criminal banking* serta biasanya dikerjakan secara teroganisir. Sebagaimana sudah disebutkan efek negatif yang dimunculkan oleh perkembangan bentuk-bentuk *cybercrime* yakni berkembangnya modus operasi oleh kejahatan tradisional yang memakai ruang virtual dalam mengerjakan tindak kejahatan. Dalam fokus *cybercrime* terhadap penelitian tersebut terletak terhadap bentuk kejahatan tradisional yang memasuki ruang virtual melalui bantuan peralatan komputer serta teknologi internet.

Contoh *cybercrime* ketika transaksi perbankan yang memakai alat Internet sebagai basis transaksi yakni sistem layanan kartu kredit serta layanan perbankan online *(online banking)*. Dalam sistem layanan yang pertama, yang perlu diwaspadai yaitu tindak kejahatan yang dikenal melalui istilah *carding*. Pada prosesnya yaitu pelaku *carding* mendapatkan data kartu kredit korban secara tidak sah *(illegal interception),* kemudian menggunakan kartu kredit tersebut dalam berbelanja di toko online *(forgery)*. Modus tersebut biasanya terjadi dikarenakan lemahnya sistem pengecekan yang dipakai dalam memastikan identitas pemesan barang di toko online.

Kegiatan yang kedua yakni perbankan online *(online banking)*. Modus yang pernah muncul di Indonesia dikenal melalui istilah *typosite* yang memanfaatkan kelengahan

nasabah yang salah mengetikkan alamat bank online yang ingin diaksesnya. Pelakunya telah mempersiapkan situs palsu yang mirip dengan situs asli bank online *(forgery)*. Jika ada nasabah yang salah ketik dan masuk ke situs bank palsu tersebut, maka pelaku akan merekam *user ID* serta *password* nasabah tersebut agar dipakai dalam mengakses ke situs yang sebenarnya *(illegal access)* bertujuan agar mengambil uang nasabah. Adapun cara Kerja Modus Pencurian Data Kartu kredit / *credit card*: 1. Membeli data nasabah dari oknum Bank senilai 20.000 rupiah. 2. Kemudian si pelaku menelpon satu persatu nasabah kartu kredit dengan mengatas-namakan pihak bank melalui alasan penawaran upgrade paket. 3. Kemudian apabila si korban sudah setuju maka mereka akan mendatangkan kurir ke pihak korban. 4. Kemudian setelah kurir datang mereka akan meminta data lengkap, seperti KTP, dan kartu kredit yang nantinya akan di scan atau bahasa umumnya di foto copy secara bolak balik ktp dan kartu kredit. 5. Kemudian setelah selesai si pelaku akan membuat duplikat kartu kredit anda dan mereka akan datang kembali kepada anda dan memberikan kartu kredit yang baru dengan datang ke tempat anda tinggal, dan si pelaku akan datang dan mengunting kartu kredit anda agar anda terlihat lebih percaya.6. Apa yang mereka gunting itu adalah kartu kredit yang palsu dan yang asli sudah mereka kantongi (Haryanto, 2015).

Sedangkan yang dimaksud dengan *fraud* dalam kartu kredit, adalah *Fraud* berarti tindakan melanggar hukum yang dilakukan seseorang atau sekelompok orang untuk mendapatkan keuntungan finansial dari penggunaan kartu kredit yang bukan menjadi hak miliknya. Dan salah satu tindakan kejahatan yang umum dilakukan adalah pencurian data kartu kredit, atau yang biasa disebut dengan istilah *phishing* (Nunuk, 2018). Orang atau komplotan yang melakukan *phishing* biasanya mengincar 4digit nomor di belakang kartu kredit, dan nomor PIN-nya. Informasi ini kemudian digunakan oleh pelaku untuk bertransaksi atas nama nasabah. terdapat empat teknik yang umum atau sering dilakukan pelaku pencurian data kartu kredit, yaitu Pelaku akan menelpon dan mengaku sebagai perwakilan dari pihak Bank atau *surveyor* yang ingin memperbaharui data kartu kredit. Modus lain yang sering digunakan adalah membuat situs belanja online palsu. Karena apabila melakukan pembayaran kartu kredit pada situs online yang tidak terpercaya, kemungkinan tujuan mereka adalah mencuri data kartu kredit. Teknik *skimming* dilakukan dengan menggunakan alat penyalin informasi. Umumnya, alat ini ditempelkan pada mesin ATM Bank. Namun juga dapat dilakukan pada mesin EDC kartu kredit dengan metode yang sama. Pelaku menggunakan sebuah alat seperti *reuter internet*, yang dapat menciptakan koneksi internet Wi-Fi palsu di gadget calon korban. Ketika calon korban telah terkoneksi dengan koneksi ini, si pelaku dapat dengan mudah melihat informasi yang tersimpan dalam *browsing history* korban.

**B. Upaya Mencegah *Cybercrime* Perbankan**

Kejahatan atau tindak pidana perbankan memiliki karakteristik yang khas, yang membedakan dengan tindak pidana lain, sehingga harus dicegah dan ditanggulangi dengan cara-cara yang khas pula. Oleh karena keadaan yang seperti itu, maka kendala selalu muncul dalam upaya mencegah dan menanggulangi kejahatan perbankan. Adapun terdapat beberapa kendala dalam penanganan tindak pidana perbankan, yang pertama adalah belum adanya kesamaan pandang tentang penggunaan dokumen fotokopi sebagai barang bukti dan dalam menetapkan undang-undang atau ketentuan yang dilanggar dalam tindak pidana bank. Kedua, tingkat pemahaman para penegak hukum terhadap kegiatan/operasional perbankan yang berbeda-beda dan belum merata serta lemahnya koordinasi dalam penanganan kasus perbankan. Kendala berikutnya adalah belum efektifnya tindak lanjut penanganan kasus yang telah diserahkan oleh Bank Indonesia kepada penyidik. Masalah yang terakhir yakni terdapat beberapa kasus yang sulit diungkapkan modus operandinya yang antara lain disebabkan oleh pesatnya kemajuan atau perkembangan teknologi informasi (Sulisrudatin, 2018).

Pencegahan dan penanggulangan tindak pidana dalam kerangka kebijakan kriminal dapat dilakukan dengan 2 (dua) cara, yaitu penal *(penal policy)* dan non penal *(non penal policy)*. *Penal policy* lebih ditekankan kepada upaya represif dari penegak hukum yang didahului dengan ketersediaan undang-undangnya. *Penal policy* menjadi tugas polisi,

jaksa, hakim, dan tentunya Bank Indonesia dalam hal pelanggaran administrasi. Sedangkan *non-penal policy,* menjadi tugas dari aparat penegak hukum, bank Indonesia, bank pemerintah maupun swasta dan masyarakat. Adapun pengaturan tindak pidana *cyber* di Indonesia juga dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana *cyber* ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Dapat diketahui selain mengatur tindak pidana *cyber* materil, UU ITE mengatur tindak pidana *cyber* formil, khususnya dalam bidang penyidikan. Pasal 42 UU ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam Undang-Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) dan ketentuan dalam UU ITE. Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kecurangan *fraud* sama halnya dengan pemalsuan, penipuan atau pemberian gambaran atau keterangan yang tidak sebenarnya dengan tujuan memperoleh keuntungan dengan menimbulkan kerugian materil bagi pihak lain. Contohnya dari bentuk kecurangan dalam perkreditan yaitu tindakan *mark up* (penggelembungan jumlah kebutuhan investasi suatu proyek untuk mendapatkan kredit yang lebih besar dari semestinya). Bentuk tindakan lain yang dapat digolongkan pada penipuan dan kecurangan dalam bidang perkreditan (*credit fraud*) yaitu tindak pidana yang diatur dalam Pasal 35 UU Nomor 42 Tahun 1999 tentang Jaminan Fidusia, yaitu tindakan debitor yang memberikan keterangan secara menyesatkan, sebagaimana diatur dalam Pasal tersebut (Jesline, 2019).

Ketentuan penyidikan dalam UU ITE berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan. Selain UU ITE, peraturan yang landasan dalam penanganan kasus *cybercrime* di Indonesia ialah peraturan pelaksana UU ITE dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.

Pencegahan dan penanggulangan kejahatan bukan sekadar terbatas pada upaya penal yang seringkali bersifat represif, akan tetapi akan lebih efektif jika dikaitkan langsung dengan karakteristik yang khas dari tindak pidana tersebut. Misalnya, pada tindak pidana perbankan, ciri yang khas adalah pada perhitungan alur masuk dan keluar uang dari nasabah, dan ilmu yang tepat untuk mengetahui kewajaran atau ketidakwajaran atas alur ini adalah akuntansi.

Penilaian yang tepat dari ilmu ini akan mencegah secara lebih dini terjadinya tindak pidana perbankan. dalam rangka penegakan hukum dan pencegahan kejahatan perbankan, maka langkah-langkah yang harus ditempuh adalah perlunya peningkatan kemampuan penyidik dalam bidang akunting dan keuangan. Lalu melakukan sistem pengawasan dari pihak bank yang efektif dan ini bisa dilakukan kalau rekruitmen pegawai lebih menekankan kepada mental idiologi. Diperlukan juga kewenangan penyidik dalam rangka menjalankan tugasnya, bukan hanya sekadar menyangkut rahasia bank. Selain itu juga diperlukan pembaharuan perundang-undangan dalam bidang ekonomi, in casu undang-undang perbankan (Sulisrudatin, 2018). Sedangkan terdapat beberapa upaya pencegahan tindak pidana, ataupun penanganan tindak pidana dimana UU ITE yang menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan computer (*cybercrime*).

## SIMPULAN

Pencegahan serta penanggulangan kejahatan perbankan tak bisa jika diserahkan hanya terhadap salah satu pihak saja dalam penegakan hukum, sehingga bukan hanya penyebab kausatif atau simptomatik yang terselesaikan, akan tetapi penyebab yang bersifat komprehensif dan dapat di atasi secara bersama-sama. Pemerintah dalam hal ini aparat hukum yang berwenang wajib mampu memberi tindakan yang tegas dan hukuman yang berat serta kewajiban bagi pelaku agar mengganti seluruh kerugian yang dialami bank maupun nasabah bank yang bersangkutan dengan demikian bagi pelaku yang terbukti

bersalah melakukan pembobolan bank akan menyadari kesalahannya lalu akan berefek bagi pihak-pihak lain supaya tidak akan mengerjakan kejahatan yang sama.

Oleh sebab itu, disarankan kepada aparat yang berwenang agar menambah pengawasannya di bidang IT, agar dapat menangkap pelaku *cybercrime* di sektor perbankan. Selain itu pemerintah juga harus memberi tindakan yang tegas dan hukuman yang berat serta kewajiban bagi pelaku agar mengganti seluruh kerugian yang dialami bank maupun nasabah bank yang menjadi korban.

## DAFTAR PUSTAKA

Akbar. (2014). Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional. jurnal ilmu Hukum jambi, Vol.VI. No.3

Arief, B. N. (2001). Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan. Bandung: Citra Aditya Bakti.

Haryanto, S. (2015). Kinerja dan Efisiensi Bank Pemerintah (BUMN) dan BUSN yang Go Publik di Indonesia. Jurnal Universitas Merdeka Malang.

Arofah, N. R., & Priatnasari, Y. (2020). Internet Banking Dan Cyber Crime: Sebuah Studi Kasus Di Perbankan Nasional. *Jurnal Pendidikan Akuntansi Indonesia*, *18*(2), 107-119.

Disemadi, H. S., & Shaleh, A. I. (2020). Banking credit restructuring policy amid COVID-19 pandemic in Indonesia. *Jurnal Inovasi Ekonomi*, *5*(02).

Disemadi, H. S., & Prananingtyas, P. (2019). Perlindungan hukum terhadap nasabah perbankan pengguna CRM (Cash Recycling Machine). *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *8*(3), 286-402.

Disemadi, H. S. (2019). Risk Management In The Provision Of People's Business Credit As Implementation Of Prudential Principles. *Diponegoro Law Review*, *4*(2), 194-208.

Jesline, A. (2019). Penganturan dantanggung awab peyedia jasa dari tindakan kebocoran data. Jurnal Unpod Repository, vol 5, Number 2: sup , page s42.

Kuwado, F. J. (2015). Waspada, Rekening Nasabah di Indonesia Rentan Dibobol. www.kompas.com. Jakarta.

Mansur, D. M. A. & Gultom. (2009). E. Cyber Law Aspek Hukum Teknologi Informasi. Bandung: Refika Aditama.

Novita I. S. (n.d). Kasus-kasus pembobolan kartu kredit yang menggemparkan, www.merdeka.com .

Nunuk, S. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. Universitas Dirgantara Marsekal. Jakarta: Suraman.

Raiza A, B. (n.d). Kartu Kredit Ditangkap, Dua Orang Diburu, www.news.com.

Shahrullah, R, S. (2014). Tinjauan Yuridis Penanganan Kejahatan Siber (Cybercrime) Di Sektor Perbankan Indonesia Dan Amerika. Journal of Judicial Review. Vol, XVI, No.2.

Soetarto dan M. Nasir, Teknologi E-Bangking dikalangan Smart Customer, http://repository.akprind.ac.id/sites/files/conference paper/2008/nasir_2127.pdf diakses pada tanggal 5 Februari 2015 Jakarta : Suraman.

Sulisrudatin, N. (2018). ANALISA KASUS CYBERCRIME BIDANG PERBANKAN BERUPA MODUS PENCURIAN DATA KARTU KREDIT. Universitas jurnal Dirgantara Marsekal Suryadarma Jakarta.

Sutianto, F.D. (2015). Cyber Crime Perbankan Makin Lihai, Kerugian Capai Rp 33 Miliar. www.detikinet.com

Widodo. (2009) Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana kerja sosial dan Pidana Pengawasan Bagi Pelak Cybercrime. Yogyakarta: Laksbang Mediatama.

Yulia, R. (2010), Viktimologi Perlindungan Hukum Terhadap Korban Kejahatan, Yogyakarta: Graha Ilmu.

Ratulangi, C. H. (2021). Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan. *Lex Privatum*, *9*(5).

Anin, M. (2020). Perlindungan Hukum Terhadap Nasabah Bank Korban Cyber Crime Dalam Internet Banking Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Iustitia Omnibus (Jurnal Ilmu Hukum)*, *1*(2), 102-113.