TINDAK KEJAHATAN SIBER DI SEKTOR JASA KEUANGAN DAN PERBANKAN[1]

Oleh: Faysal Banua Suwiknyo[2]
Tonny Rompi[3]
Harly Stanly Muaja[4]

ABSTRAK

Tujuan dilakukannya penelitian ini adalah untuk mengetahui bagaimana bentuk-bentuk kejahatan yang termasuk sebagai kejahatan di bidang siber dan bagaimana penerapan hukum pidana terhadap para pelaku kejahatan siber di sektor jasa keuangan dan perbankan di mana dengan metode penelitian hukum normatif disimpulkan: 1. Kejahatan siber (*cyber crime*) dilakukan oleh orang baik secara sendiri maupun berkelompok yang benar-benar ahli dalam peretasan, ahli dalam menggunakan komputer sebagai sarana/alat untuk melakukan kejahatan, sehingga menurut para ahli bentuk-bentuk kejahatan siber (*cybercrime*) itu secara umum adalah berupa pencurian identitas, *spionage cyber,* pemerasan *cyber*, pencurian data perusahaan, dan *carding*. Sedangkan menurut UU No. 11 Tahun 2008 yang dirobah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, bentuk-bentuk kejahatan siber (*cyber crime*) adalah tindak pidana yang berhubungan dengan aktivitas *illegal*, tindak pidana yang berhubungan dengan gangguan (interferens), tindak pidana memfasilitasi perbuatan yang dilarang, dan tindak pidana pemalsuan informasi atau dokumen elektronik. 2. Tindak kejahatan siber (*cyber crime*) di sektor jasa keuangan dan perbankan adalah *social engineering* dan *skimming*. Kedua bentuk kejahatan siber ini dilakukan dengan teknik menipu atau penipuan, penggelapan dan pencurian. Oleh karena itu penerapan hukum pidana terhadap para pelaku kejahatan siber di sektor jasa keuangan dan perbankan itu oleh para hakim banyak menggunakan pasal-pasal yang ada dalam KUHP yaitu Pasal 64 tentang perbuatan berlanjut, karena pelaku melakukannya berkali-kali, Pasal 362 tentang Pencurian, Pasal 363, pencurian yang dilakukan oleh lebih dari satu orang dan Pasal 378 tentang penggelapan.

Kata kunci: kejahatan siber; jasa keuangan; perbankan;

PENDAHULUAN

A. Latar Belakang Masalah

Kejahatan bukanlah konsep baru dalam sejarah peradaban manusia. Sejak manusia diciptakan yang dimulai dengan tindakan pembangkangan iblis terhadap perintah Allah untuk memberi penghormatan makhluk ciptaan Allah lainnya yang disebut manusia. Pembangkangan ini kemudian diteruskan dengan janji iblis untuk selalu menggoda manusia hingga akhir Zaman.[5] Konflik interest antara manusia dan iblis ini dapat dipandang sebagai embrio kejahatan. Bermula dari perasaan iri, sombong, dan dengki, kejahatan itu dimulai. Pada tahapan perkembangannya kemudian, modus operandi kejahtan bergerak maju seiring perkembangan peradaban manusia. kejahtan dan eksistensi masyarakat menjadi 'dua sisi mata uang' yang saling terkait sehingga Lacassagne mengatakan bahwa masyarakat mempunyai penjahat sesuai dengan jasanya.[6] Bermacam ragam kejahatan muncul seiring dengan perkembangan zaman dan kemajuan ilmu pengetahuan serta teknologi, begitu juga dengan kejahatan siber (*cyber crime*).

B. Rumusan Masalah

1. Bagaimana bentuk-bentuk kejahatan yang termasuk sebagai kejahatan di bidang siber?
2. Bagaimana penerapan hukum pidana terhadap para pelaku kejahatan siber di sektor jasa keuangan dan perbankan?

C. Metode Penelitian

Metode pendekatan yang digunakan adalah yuridis normatif.

PEMBAHASAN

A. Bentuk-Bentuk Kejahatan Siber

[1] Artikel Skripsi
[2] Mahasiswa pada Fakultas Hukum Unsrat, NIM : 14071101376
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Maskun, *Kejahatan Siber (Cyber crime) Suatu Pengantar,* Kencana, Prenata Media Group, Jakarta, 2013, hlm. 42,
[6] Agus Raharjo, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahtan Berteknologi*, Citra Aditya, Banung, 2002, hlm. 29 – 30.

Kejahatan siber atau *cyber crime* adalah tindak kejahatan yang dilakukan secara *online*. Kejahatan ini tidak mengenal waktu dan tidak pilih-pilih target. Bisa terjadi pada individu atau perusahaan dimanapun berada. Tujuan kejahatan siber sendiri beragam. Bisa sekedar iseng, sampai kejahatan serius yang merugikan korbannya secar finansial.[7] Pada praktiknya, kejahatan dunia maya bisa dilakukan seorang diri atau sekelompok orang. Para pelaku kejahatan dunia maya tentu adalah orang yang sudah ahli dalam berbagai teknik peretasan. Bahkan tidak jarang sebuah aksi kejahatan siber (*cyber crime*) dilakukan dari berbagai tempat berbeda di waktu bersamaan.

Begitu banyak ragam bentuk-bentuk kejahatan siber yang masih sering dijumpai saat ini yaitu:[8]

1. Pencurian identitas

Sesuai namanya, pencurian identitas adalah jenis kejahatan siber (*cyber crime*) berupa aksi perampokan identitas. Pencurian identitas pelaku akan melakukan teknik peretasan pada website korban, mereka akan mengakses situs *web server* untuk mendapatkan informasi pribadi yang tersimpan. Pencurian identitas akan cenderung menyasar toko *online*, keanggotaan website dan jenis *website* lain yang menggunakan data pelanggan dalam proses layanannya. Selain itu pencurian identitas juga dapat terjadi saat kita mengakses situs abal-abalan. Hal ini dapat terjadi saat kita memberikan data pribadi padahal situs itu sebenarnya milik peretas. Contoh kasus yang sering terjadi adalah perampokan identitas menggunakan sayembara *online*, tergiur iming-iming hadiah yang besar, korban akan mengisi data diri di sebuah situs, ternyata undian sayembara tidak pernah ada, namun data diri korban sudah terlanjur dimiliki oleh peretas/penjahat siber.[9]

2. *Carding*[10]

Carding adalah jenis kejahatan siber (*cyber crime*) yang berupa pembobolan kartu kredit. *Carding* adalah salah satu jenis kejahatan siber yang masih sering dilakukan. Kasus terakhir bahkan sempat terkait dengan beberapa orang terkenal. Pelaku *Carding* melakukannya dengan berbagai cara seperti: *phising*, memutus *malware* di toko *online* atau membeli informasi secara gelap dari internet. Dampak dari *carding* ini kadang kala tidak disadari oleh korban. Jika tidak cepat disadari, korban pemilik kartu kredit akan dan harus membayar tagihan besar atas belanja yang tidak dilakukannya.

3. Pencurian Data Perusahaan[11]

Pencurian data perusahaan mirip dengan pencurian identitas, bedanya jenis kejahatan siber ini menyasar data perusahaan. Pelaku meretas situs perusahaan, kemudian mengisi data-data yang penting. Data perusahaan yang berhasil didapatkan bisa digunakan atau dimanfaatkan untuk kepentingan pribadi, misalnya untuk bisa mengaksesnya tanpa hak. Bisa juga data tersebut dijual di pasar gelap dengan harga tinggi. Bentuk kejahatan siber ini pernah mencoba perusahaan-perusahaan besar, salah satunya adalah 'Canva'. Situs perusahaan ini, perusahaan desain grafis, berhasil diretas sehingga 139 juta data pelanggan terancam. Artinya dalam satu aksi saja, pencuri bisa mendapatkan banyak data untuk digunakan melakukan kejahatan khususnya kejahatan siber.[12]

4. Pemerasan *Cyber*[13]

Istilah pemerasan *cyber* digunakan untuk kejahatan online yang menimpa perusahaan atau pribadi. Modusnya, pelaku akan meminta uang sebagai tebusan atas data penting yang telah dicuri. Kasus kejahatan siber (*cyber crime*) berupa pemerasan yang marak saat ini adalah *ransomware. Malware* ini masuk ke perangkat dari korban dan mengendalikan data di dalamnya. Pemilik tidak dapat mengakses data tersebut tanpa menggunakan sandi dari pelaku kejahatan. Dan biasanya untuk mendapatkan sandi tersebut biasanya pelaku akan meminta uang tebusan terlebih dahulu. Banyak perusahaan terkenal di dunia yang menjadi korban kejahatan siber ini. Misalnya Nokia, Domino dan Freedly. Bahkan pada kasus Domino, peretas meminta uang tebusan 30.000 Euro agar data 650.000 pelanggan Domino tidak akan disebarluaskan.

5. Spionase *Cyber*[14]

[7] *Mengenal Cyber Crime, Kejahatan Online Yang Wajib Diwaspadai*, *Op-Cit.*
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid*
[11] *Ibid.*
[12] *Ibid.*
[13] *Ibid*

*Cyber spionage*adalah jenis kejahatan siber yang memata-matai target tertentu, seperti lawan politik, kompetitor suatu perusahaan atau pejabat negara lain. Pelaku menggunakan teknologi canggih untuk memata-matai secara *online*. Spionase *cyber* biasa dilakukan dengan memanfaatkan *spyware*. Dengan aplikasi yang ditanam di komputer korban, semua aktivitas dan data penting bisa diakses tanpa disadari. Sebagai contoh, kejahatan spionase *cyber* ini pernah menimpa Barrack Obama, saat itu *spyware* digunakan untuk mengukur data yang terkait kebijakan luar negeri Amerika.

Bentuk-bentuk kejahatan siber ini biasa dilakukan pelaku kejahatan dengan melakukan aksi sebagai berikut:[15]

a) Serangan *Malware*

Malware adalah aksi kejahatan siber (*cyber crime*) dengan menggunakan perangkat lunak yang menyusup ke perangkat korban. Aksi ini sering berhasil mencapai tujuan karena korban tidak tahu ada serangan *malware*, artinya, aksi kejahatan bisa dilakukan dengan leluasa. Biasanya, *malware* masuk melalui email, pesan di *instan messaging* atau saat akses ke *website* yang berbahaya. Tidak jarang juga *malware* masuk melalui tema atau *plugin Wordpress* yang diinstal ke sistem situs korban. Saat berada di perangkat korban, *malware* bisa melakukan apapun sesuai program yang dijalankan. Misalnya, data, memata-matai perilaku *online* korban hingga data yang diinginkan.

b) Phishing[16]

Kejahatan siber jenis ini masih menjadi aksi kejahatan siber favorit para peretas. Alasannya, kejahatan online masih efektif, terutama untuk perampokan identitas. Menurut sebuah laporan bahwa aksi kejahatan siber (*cyber crime*) yaitu 67% bermula dari *phishing.* Data yang menjadi tujuan phishing adalah berupa data pribadi (nama, usia dan alamat), data akun (nama pengguna dan sandi) dan data finansial (nomor kartu kredit dan kata sandi). Langkah *phishing* kerap berhasil karena pelaku *phishing* menyamar menjadi pihak yang peduli atau lembaga resmi, sehingga korban tidak merasa curiga. Contoh kasus *phishing* yang terkenal adalah penggunaan *Paypal.* Pelaku mengirimkan *email* kepada korban dengan berpura-pura sebagai pihak *Paypal*. Dalam isi *email* tersebut, pelaku menyatakan bahwa korban telah menyebabkan sebagai akibat dari kebijakan-kebijakan. Lewat *email* tersebut, pelaku meminta korban untuk meminta perbarui akun mereka. Sebuah tautan yang diberikan pelaku akan mengarahkan korban ke situs palsu, ketika korban memasukkan data diri sesuai petunjuk, pelaku berhasil mendapatkan informasi yang diinginkan.

c) Deface Website[17]

Deface adalah upaya mengubah tampilan sebuah situs situs web tanpa hak. Aksi kejahatan siber (*cyber crime*) ini pernah heboh di Indonesia karena menimpa *website* lembaga pemerintah yakni Komisi Pemilihan Umum (KPU). Dalam aksinya, pelaku yang menyerang situs resmi KPU Kabupaten Seluma membuat tampilan berubah. Pelaku juga menyatakan bahwa situs tersebut telah berhasil diretas oleh suatu kelompok. Selain mengubah tampilan situs, aksi kejahatan siber ini juga sering digunakan untuk mengarahkan korban ke situs lainnya. Misalnya, aksi *deface* pada *website Google* di Romania. Meskipun aksi ini sendiri disangkal pihak *Google*, pengunjung saat itu tidak dapat mengakses *google.ro.*

d) Serangan *DDoS*[18]

Serangan DDoS adalah aksi kejahatan siber dengan target serangan ke *server*. Caranya, dengan membuat lalu lintas sebuah *server* yang terlalu tinggi sampai tidak bisa mengatasi permintaan akses dari pengguna. Aksi DDoS berupaya membuat situs *web server*, *down,* sehingga pengunjung tidak dapat mengaksesnya. Kenyataannnya, DDoS sendiri merupakan suatu salah satu serangan yang populer digunakan oleh *hacker*. Alasannya, teknik DDoS sederhana untuk dijalankan. Serangan DDoS sangat mengancam reputasi *online* yang dibangun. Kepercayaan konsumen terhadap sebuah bisnis yang mengalami *down of source* akan hilang. Contohnya, *British Broadcasting Coorporation* (BBC), salah satu media terbesar di dunia, serangan yang terjadi mengakibatkan semua layanan BBC hampir lumpuh, seluruh *domain* milik BBC tidak bisa diakses. Layanan *on-demand* dan radio juga ikut mati.

[14] *Ibid.*
[15] *Ibid.*
[16] Ibid.
[17] *Ibid.*
[18] *Ibid.*

e) Peretasan

Hacking adalah istilah kejahatan siber yang cukup umum. Aksi ini dilakukan dengan cara mengakses sistem komputer korban tanpa hak. Para *hacker* akan menggunakan keterampilan yang dimiliki untuk melakukan berbagai aksi kejahatan siber, mulai merusak sistem, data pribadi, hingga mengekspos data yang diperoleh ke publik. Aksi *hacking* tidak selamanya bertujuan mendapatkan keuntungan finansial. Banyak juga *hacker* yang hanya sekedar untuk memamerkan keahlian yang dimiliki. Contohnya, aksi *hacking* yang kerap terjadi adalah pembobolan kata sandi. Langkah inilah yang menjadi titik awal *hacker* melakukan kejahatan selanjutnya. Beberapa waktu yang lalu, dua media besar di Indonesia pernah menjadi korban *hacking*. Para *hacker* berhasil menembus sistem keamanan situs *web* media tersebut dan berhasil membuat beberapa berita yang pernah dimuat.

Ari Juliano Gema mengatakan bahwa kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam praktiknya dikelompokkan dalam beberapa bentuk sebagai berikut:[19]

1. *Unauthorized acces to computer system and service,* yaitu kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa isin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud untuk sabotase ataupun pencurian informasi penting dan rahasia. Salah satu contoh: pada tahun 1999, ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di level internasional, beberapa *website* milik pemerintah Republik Indonesia dirusak oleh *hacker*.[20]
2. *Illegal cotents,* yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis dan dianggap melanggar hukum atau mengganggu ketertiban umum.[21] Cotohnya: pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, pemuatan hal-hal yang berbau pornografi, pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintah yang sah.
3. *Data forgery,* yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi 'salah ketik' yang pada akhirnya akan menguntungkan pelaku.[22]
4. *Cyber spionage,* yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan kepada saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi.[23]
5. *Cyber Sabotage and Extortion,*[24]yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb* (suatu program yang dibuat dan dapat digunakan oleh pelakunya sewaktu-waktu atau tergantung dari keinginan si pelaku), virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.
6. *Offence against intellectual property,* yaitu kejahatan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Contohnya: peniruan tampilan *web page* suatu situs

[19]Ari Juliano Gema, *Cyber crime; Sebuah Fenomena di Dunia Maya, Op-Cit.*
[20]*Kompas*, 11 Agustus 1999.
[21] Ari Juliano Gema, *Loc-Cit.*
[22]*Ibid,* hlm. 52.
[23]*Ibid.*
[24]*Ibid*, hlm. 53.

milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.[25]

7. *Infringements of privacy,* yaitu kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia.[26] Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara material maupun imaterial, seperti nomor kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi dan sebagainya.

UU No. 11 Thaun 2008 yang dirubah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, tidak memberikan definisi tentang kejahatan siber (*cybercrime*), tetapi membaginya menjadi beberapa pengelompokkan yang mengacu pada *Convention on Cybercrime* sebagai berikut:[27]

1. Tindak Pidana yang berhubungan dengan aktivitas *illegal*, yaitu:
   a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten *illegal*, yang terdiri dari:
      - kesusilaan {Pasal 27 ayat (1)};
      - perjudian {Pasal 27 ayat (2)};
      - penghinaan dan/atau pencemaran nama baik {Pasal 27 ayat (3)};
      - pemerasan dan/atau pengancaman {Pasal 27 ayat (4)};
      - berita bohong yang menyesatkan dan merugikan konsumen {Pasal 28 ayat (1)};
      - menimbulkan rasa kebencian berdasarkan SARA {Pasal 28 ayat (2)};
      - mengirimkan informasi yang berisi ancaman kekrasan atau menakut-nakuti yang ditujukan secara pribadi {Pasal 29}.
   b. Dengan cara apapun melakukan akses *illegal* {Pasal 30}.
   c. Intersepsi atau penyadapan *illegal* terhadap informasi atau dokumen elektronik dan sistem elektronik {Pasal 31}.
2. Tindak pidana yang berhubungan dengan gangguan (*interferensi*), yaitu:
   a. Gangguan terhadap informasi atau dokumen elektronik (*data interference* – Pasal 32)
   b. Gangguan terhadap sistem elektronik (*system interference* – Pasal 33).
3. Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34).
4. Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35).
5. Tindak pidana tambahan (*accessoir* Pasal 36).
6. Pemberatan-pemberatan terhadap ancaman pidana (Pasal 52).

B. Penerapan Hukum Pidana Terhadap Pelaku Kejahatan Siber di Sektor Jasa Keuangan dan Perbankan

Kejahatan siber (*cybercrime*) terjadi di Indonesia sejak tahun 1983, terutama di bidang perbankan.[28] Dalam tahun-tahun berikutnya sampai sekarang ini, di Indonesia banyak terjadi kejahatan siber (*cybercrime*), misalnya pembajakan komputer, cracking, penggunaan kartu kredit pihak lain secara tidak sah (*carding*), pembobolan bank (*banking fraud*), pornografi, termasuk kejahatan terhadap nama domain (*domain name*).[29]

Bentuk-bentuk kejahatan siber (*cybercrime*) di Indonesia dapat dikaitkan dengan ketentuan hukum pidana Indonesia, baik ketentuan KUHP maupun ketentuan pidana dalam peraturan perundang-undangan di luar KUHP yaitu UU No. 11 Tahun 2008 Jo UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Meskipun demikian, ada perbedaan konsepsi antara hukum pidana Indonesia dengan karakteristik kejahatan siber (*cybercrime*). Beberapa terminologi KUHP sulit digunakan sebagai dasar hukum untuk mengadili kejahatan siber (*cybercrime*), misalnya pengertian 'di depan umum' yang disamakan

[25] *Ibid*.
[26] *Ibid,* hlm. 54.
[27] Josua Sitompul, *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*, PT Tatanusa, 2012.
[28] Aloysius Wisnubroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Universitas Atmajaya, Yogaykarta, 1999, hlm 46-47.
[29] Widodo, *Op-Cit*, hlm. 45.

dengan pengertian 'di dalam internet', pengertian 'memasuki pekarangan tertutup' sebagimana diatur dalam KUHP untuk mengadili kasus 'memasuki ruang (*space*)' milik pihak lain di internet (*illegal access*).

Tindak kejahatan siber (*cybercrime*) di sektor jasa keuangan dan perbankan secara umum terbagi atas dua (2) jenis yakni:[30]

1. *Sosial engineering,* adalah manipulasi psikologis seseorang dengan tujuan untuk mendapatkan informasi tertentu dengan cara menipu secara halus, baik disadari atau tidak melalui telepon atau berbicara langsung.
2. *Skimming,* adalah tindakan pencurian informasi dengan cara menyalin informasi yang terdapat pada strip magnetik kartu debit atau kredit secara *illegal*. Metode *skimming* merupakan metode yang digunakan untuk mencuri informasi nasabah pada saat bertransaksi menggunakan ATM.[31] Dalam menjalankan tindak kejahatan ini terdapat tiga (3) alat utama yang digunakan yaitu: *skimmer, hidden camera* dan *keypad*. Alat *skimmer* berfungsi untuk merekam aktivitas nasabah dalam menggunakan mesin ATM, alat ini mampu merekam strip elektromagnetik yang ada pada kartu korban pada saat kartu dimasukkan ke mesin ATM. *Hidden camera* dan *keypad* digunakan untuk merekam aktivitas korban pada saat melakukan penginputan PIN pada mesin ATM.

Adapun teknik dasar memperoleh informasi dengan modus *social engineering* bermacam-macam, ada tiga (3) yang paling lumrah yakni:[32]

1. *Phishing*, teknik *phising* digunakan para pelaku dengan mengelabui atau memanipulasi para pemilik rekening bank sehingga mereka memberikan data dan informasi yang bisa digunakan untuk mengakses akun perbankan milik nasabah.[33] Pengelabuan yang dilakukan untuk mendapatkan informasi rahasia seperti *password* dengan menyamar sebagai orang atau bisnis terpercaya dalam sebuah komunikasi elektronik. Saluran yang digunakan sebagai *email*, layanan pesan instan (SMS), atau penyebaran link palsu di internet untuk mengarahkan korban ke *website* yang telah dirancang untuk menipu.[34]
2. *Vishing,* yakni upaya penipu melakukan pendekatan terhadap korban untuk mendapatkan informai atau mempengaruhi korban untuk melakukan tindakan. Biasanya komunikasi dilakukan melalui telepon.[35]
3. *Impersonation,* yakni upaya penipu berpura-pura menjadi orang lain dengan tujuan untuk mendapatkan informasi rahasia.

Adapun modus *social engineering* yang sering dilakukan penipu di antaranya:[36]

1. *Fraud internet banking* dan transaksi *online* menggunakan kartu kredit/kartu debit, yakni pelaku mengaku sebagai pegawai bank yang menginformasikan adanya perubahan biaya layanan SMS/internet banking, pemberian bonus pulsa, pembagian hadiah undangan, dan lain-lain. Pelaku juga melakukan penipuan penawaran pinjaman *online* dengan bunga murah.
2. *Contact centre bank,* yakni penipu memanipulasi mesin ATM agar korban gagal bertransaksi dan kartu tertelan di mesin. Pada saat bersamaan, anggota tim penipu *standby* disekitar ATM untuk mengarahkan korban menghubungi nomor *call centre* palsu. Tim yang berpura-pura menjadi *call centre* palsu memberitahukan bahwa ATM telah diblokir, kemudian meminta korban memberikan identitas pribadi termasuk nomor PIN ATM. Pelaku yang berada disekitar korban kemudian mengambil

[30] Farodilah Muqoddam, *Mengenal Modus Kejahatan Keuangan, Definisi Skimming, Phishing dan Vishing,* 2019, diakses darim.bisnis.com pada tanggal 2 Oktober 2020.

[31] Arifianto. T, *Penerapan Fingerprint Recognition Dengan Metode Learning Vector Quantization (LVQ) dalam Automatic Teller Machine (ATM)*, Jurnal SPIRIT, 2018, hlm. 2

[32] *Ibid.*

[33] *Wasapadai Modus Operandi Kejahatan Siber Perbankan*, 2019, diakses dari dialogpublik.com pada tanggal 31 Oktober 2020

[34] Farodilah Muqoddam, *Loc-Cit.*

[35] *Ibid.*

[36] *Ibid.*

kartu ATM milik korban yang tertelan di mesin.

3. *Fraud* SMS penipuan, korban menerima konten SMS yang berisi iming-iming hadiah, diskon, bonus pulsa, paket tour wisata, pinjaman *online* dan lainnya. Dengan dalih mencairkan hadiah, korban akan dipancing ke mesin ATM dan diarahkan untuk mengikuti instruksi yang diberikan pelaku seperti melakukan transfer dana atau *top-up* saldo *e-commerce.*

Selain apa yang sudah disebutkan di atas, bentuk-bentuk kejahatan siber di sektor jasa keuangan dan perbankan, masih ada bentuk yang lain yakni:

1. Pencurian identitas nasabah, bisa dilakukan melalui aplikasi apa saja. Salah satu sasaran pencurian adalah melalui *open banking. Open banking* adalah sistem penyedia jasa interaksi antara nasabah dengan lembaga keuangan. Sistem ini bisa dibaca oleh pelaku pencurian dengan '*skimming*' atau menyadap data profil nasabah.[37]
2. *Skimming*, teknik ini dilakukan pelaku dengan cara mengkloning kartu ATM milik nasabah ke dalam kartu ATM kosong. Caranya, para pelaku memasang *wifi pocket oruter* disertai kamera yang dimodifikasi menyerupai penutup PIN pada mesin-mesin ATM untuk mencuri PIN nasabah sebelum kemudian diduplikasi.[38]
3. *Malware,* merupakan singkatan dari *malicious software,* yang artinya *software* yang tidak diinginkan dalam sistem komputer.[39] *Malware* dapat mencakup dari semua perangkat lunak yang digunakan untuk mengukur, memanipulasi atau bahkan memata-matai sebuah sistem. *Malware* merupakan istilah yang digunakan untuk mendeskripsikan perangkat lunak berbahaya. *Malware* dapat disebarkan melalui beberapa metode. Sebagian besar adalah melalui jaringan internet, *email*, pesan pribadi, atau halaman situs *web.*[40] *Malware* sangat sulit untuk dideteksi oleh sistem komputer. Karena ada dua (2) jalur yang menyebabkan sistem komputer terkena oleh *malware* yaitu melalui *USB Drive* dan melalui jaringan internet. Sampai sekarang ini malware masih menjadi ancaman serius bagi dunia maya secara global.
4. *Hacking,* adalah istilah kejahatan siber yang cukup umum. Aksi ini dilakukan dengan cara mengakses sistem komputer korban tanpa hak. Para *hacker* akan menggunakan keterampilan yang dimiliki untuk melakukan berbagai aksi kejahatan publik. Aksi *hacking* tidak selamanya bertujuan mendapatkan keuntungan finansial. Banyak juga *hacker* yang hanya sekedar untuk memamerkan keahlian yang dimiliki. Contohnya, aksi *hacking* yang kerap terjadi adalah pembobolan kata sandi. Langkah inilah yang menjadi titik awal *hacker* melakukan kejahatan selanjutnya. Beberapa waktu yang lalu, dua media besar di Indonesia pernah menjadi korban *hacking*. Para *hacker* berhasil menembus sistem keamanan situs *web* media tersebut dan berhasil membuat beberapa berita yang pernah dimuat.

Melihat pada bentuk-bentuk kejahatan siber di sektor jasa keuangan dan perbankan di atas, maka ada 3 bentuk kejahatan siber yang penerapan hukumnya dilakukan dengan Kitab Undang-Undang Hukum Pidana, yaitu:[41]

1. Kasus *Unauthorized Transfer Payment* di Bank Negara Indonesia (BNI) cabang New York *Agency* (Tahun 1986).

Dalam kasus ini, Pengadilan Jakarta menjatuhkan pidana terhadap terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 ayat (1) huruf d KUHP, yaitu pencurian yang dilakukan oleh lebih dari dua (2) orang secara bersama-sama. Putusan tersebut dikuatkan oleh Putusan Pengadilan Tinggi

[37] Azizah Reftika Wulandari, *Mengulik Kiat Bank Atasi Kejahatan Siber,* diakses dari lokadata.id pada tanggal 31 Oktober 2020.

[38] *Ibid.*

[39] Kurniawan A and Prayudi. Y, *Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics, Hadfex (Hacking and Digital Forensics Exposed),* 2014, hlm. 4 – 5.

[40] *Apa itu malware? Pengertian dan Cara Mengatasinya*, diakses dari www.niagahoster,co.id pada tanggal 2 Oktober 2020.

[41] Widodo, *Op-Cit,* hlm. 95 – 96.

Jakarta dan Putusan Mahkamah Agung Republik Indonesia.[42]

Ketentuan Pasal 363 ayat (1) KUHP berbunyi sebagai berikut:

Diancam dengan pidana penjara paling lama tujuh tahun: huruf d. pencurian yang dilakukan oleh dua orang atau lebih.

Dalam kasus ini, memindahkan data komputer ke tempat lain dapat dikategorikan dalam pengertian 'mengambil' sebagaimana dimaksud KUHP, meskipun data komputer yang dipindahkan tidak mengakibatkan hilangnya data asli.

Dalam kasus-kasus lain, juga terjadi penafisran ekstensif, penafsiran yang memperluas arti, yaitu terhadap penegrtian 'rumah, ruangan, pekarangan tertutup', sehingga perbuatan seseorang dalam memasuki program komputer yang dioperasikan dalam suatu jaringan dapat dikategorikan sebagai perbuatan memaksa memasuki rumah atau ruangan, atau pekarangan tertutup secara melawan hukum sebagaimana diatur dalam KUHP.

2. Kasus Penarikan Hasil Setoran Warkat Fiktif di PT Bak Vali Jakarta (Tahun 1989)

Dalam kasus ini, Pengadilan Negeri Jakarta Barat menjatuhkan pidana penjara kepada terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 362 KUHP, yaitu pencurian biasa.[43]

Ketentuan Pasal 362 KUHP berbunyi sebagai berikut:

Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah.

Dalam mengadili perkara ini, hakim melakukan penafsiran ekstensif terhadap penegertian 'mengambil' dan 'barang'.

3. Kasus Manipulasi Data Saldo pada *Master File* Bank Danamon Cabang Glodog Plaza (Tahun 1990)

Pengadilan Negeri Jakarta Barat menjatuhkan pidana penjara kepada terdakwa karea terdakwa secara sah dan meyakinkan melanggar Pasal 363 ayat (1) huruf e KUHP, *juncto* Pasal 64 ayat (1) KUHP, yaitu melakukan pencurian dalam keadaan memberatkan yang dilakukan berulang kali sebagai perbuatan berlanjut. Putusan tersebut dikuatkan oleh putusan Pengadilan Tinggi dan Putusan Mahkamah Agung.[44]

Dalam kasus ini, pengertian 'kunci palsu' ditafsirkan secara ekstensif, sehingga kode akses (*password*) dapat dikategorikan dalam pengertian kunci palsu sebagaimana diatur dalam KUHP.

Selain pasal-pasal dalam KUHP yang disebutkan di atas, maka penerapan hukum terhadap pelaku kejahatan siber di sektor jasa keuangan dan perbankan adalah juga sebagaimana yang diatur dalam Pasal 378 dan Pasal 362 (tentang kasus *Carding* karena pelaku melakukan penipuan seolah-olah ingin membayar, dengan kartu kredit hasil curian). *Carding* menurut versi POLRI meliputi:[45]

1. mendapatkan nomor kartu kredit (CC) dari tamu hotel, khususnya orang asing.
2. mendapatkan nomor kartu kredit melalui kegiatan chatting di internet.
3. melakukan pemesanan barang ke perusahaan di luar negeri dengan menggunakan jasa internet.
4. mengambil dan memanipulasi data di internet.
5. memberikan keterangan palsu, baik pada waktu pemesanan maupun pada saat pengambilan barang di Jasa Pengiriman.

Carding (pelakunya biasa disebut *carder*) adalah kegiatan melakukan transaksi *e-commerce* dengan nomor kartu kredit palsu atau curian.

PENUTUP

A. Kesimpulan

1. Kejahatan siber (*cyber crime*) dilakukan oleh orang baik secara sendiri maupun berkelompok yang benar-benar ahli dalam peretasan, ahli dalam menggunakan komputer sebagai sarana/alat untuk melakukan kejahatan,

[42] *Ibid,* hlm. 95.

[43] *Ibid.*

[44] Widyopramono, *Kejhatan di Bidang Komputer*, Pustaka Sinar Harapan,1994, hlm. 67.

[45] Arifiyadi Teguh, *Menjerat Pelaku Cyber Crime dengan KUHP*, Pusat Data Departemen Komunikasi dan Informatika, 2008, diakses dari depkominfo.go.id pada tanggal 2 November 2020.

sehingga menurut para ahli bentuk-bentuk kejahatan siber (*cybercrime*) itu secara umum adalah berupa pencurian identitas, *spionage cyber,* pemerasan *cyber*, pencurian data perusahaan, dan *carding*. Sedangkan menurut UU No. 11 Tahun 2008 yang dirobah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, bentuk-bentuk kejahatan siber (*cyber crime*) adalah tindak pidana yang berhubungan dengan aktivitas *illegal*, tindak pidana yang berhubungan dengan gangguan (interferens), tindak pidana memfasilitasi perbuatan yang dilarang, dan tindak pidana pemalsuan informasi atau dokumen elektronik.

2. Tindak kejahatan siber (*cyber crime*) di sektor jasa keuangan dan perbankan adalah *social engineering* dan *skimming*. Kedua bentuk kejahatan siber ini dilakukan dengan teknik menipu atau penipuan, penggelapan dan pencurian. Oleh karena itu penerapan hukum pidana terhadap para pelaku kejahatan siber di sektor jasa keuangan dan perbankan itu oleh para hakim banyak menggunakan pasal-pasal yang ada dalam KUHP yaitu Pasal 64 tentang perbuatan berlanjut, karena pelaku melakukannya berkali-kali, Pasal 362 tentang Pencurian, Pasal 363, pencurian yang dilakukan oleh lebih dari satu orang dan Pasal 378 tentang penggelapan.

B. Saran

1. Karena begitu banyaknya bentuk-bentuk kejahatan siber (*cyber crime*) dimana bentuk-bentuk kejahatan itu dilakukan oleh orang-orang yang benar-benar ahli (*expert*) dalam penggunaan komputer atau yang lebih dikenal dengan *hacker*, maka seharusnya pemerintah merangkul para *hacker* ini agar mereka menggunakan keahliannya untuk menangkal kejahatan siber.
2. Tindak kejahatan siber disektor jasa keuangan dan perbankan semakin sering terjadi dan sangat merugikan nasabah, oleh karenanya para pelaku kejahatan siber harus mendapat hukuman yang berat agar mereka menjadi jera untuk melakukannya lagi. Dalam peraturan perundang-undangan harus dengan tegas untuk mengatur ancaman hukuman yang berat.

DAFTAR PUSTAKA

Arief Barda Nawawi , *Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2002

A Kurniawan and Prayudi. Y, *Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics, Hadfex (Hacking and Digital Forensics Exposed),* 2014.

Judhariksawan, *Pengantar Hukum Telekomunikasi,* Rajawali Press, Jakarta, 2005.

Kartanagara, Satochid*Hukum Pidana II, Delik-Delik Khusus,* Balai Lektur Mahasiswa, Jakarta, Tanpa Thn.

Kusumah Mulyana. W, *Kejahatan, Penjahat dan Reaksi Sosial*, Akumni, Bandung, 1983

Maskun, *Kejahatan Siber (Cyber crime) Suatu Pengantar,* Kencana, Prenata Media Group, Jakarta, 2013

Prodjodikoro Wirjono, *Tindak-Tindak Pidana Tertentu di Indonesia***,** RefikaAditama, Bandung

Raharjo Agus, *Cyber Crime; Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* Citra aditya Bakti, Jakarta, 2006.

Safitri Indra, *Tindak Pidana di Dunia Cyber, Insider, Legal Journal From Indonesian Capital and Investment Market*, diakses hhtp://business.fortunecity.com pada tanggal 27 Oktober 2020.

Sitompul Josua, *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*, PT Tatanusa

Soekanto Soerjono dan Sri Mamudji, *Penelitian Hukum Normatif; Suatu Tinjauan Singkat,* PT Raja Grafindo Persada, Jakarta, 2003

T Arifianto, *Penerapan Fingerprint Recognition Dengan Metode Learning Vector Quantization (LVQ) dalam Automatic Teller Machine (ATM)*, Jurnal SPIRIT, 2018

Wahid Abdul dan Moh, Labib,*Kejahatan Mayantara (Cyber crime),*RefikaAditama, Jakarta, 2005.

Widyopramono Hadi Widjojo, *Cybercrimes dan Pencegahannnya*, Jurnal Hukum Teknologi,

Fakultas Hukum Universitas Indonesia, Jakarta, 2005

William Wiebe, *Tindak Kejahatan Melalui Komputer,* Seminar, Makassar, 2000.

Widodo, *Hukum Pidana di Bidang Teknologi Informasi; Cybercrime Law: Telaah Teoritik dan Bedah Kasus,* Aswaja Pressindo, Yogyakarta, 2011

Wisnubroto Aloysius, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Universitas Atmajaya, Yogaykarta, 1999

Widyopramono, *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan,1994.

Sumber Internet

Azizah Reftika Wulandari, *Mengulik Kiat Bank Atasi Kejahatan Siber,* diakses dari lokadata.id pada tanggal 31 Oktober 2020.

Farodilah Muqoddam, *Mengenal Modus Kejahatan Keuangan, Definisi Skimming,*

Phishing dan Vishing, 2019, diakses darim.bisnis.com pada tanggal 2 Oktober 2020.

Gema Ari Juliano, *Cyber crime: Sebuah Fenomena di Dunia Maya*, diakses dari www.theceli.com pada tanggal 27 Oktober 2020.

Teguh Arifiyadi, *Menjerat Pelaku Cyber Crime dengan KUHP*, Pusat Data