TINDAK PIDANA PENCURIAN DATA NASABAH DALAM BIDANG PERBANKAN SEBAGAI *CYBER CRIME*

Putri Wahyu Widayanti

Fakultas Hukum Universitas Sebelas Maret
Jl. Ir Sutami No.36A, Surakarta
Email: Putriwahyu728@gmail.com

Naskah dikirim: 16/03/2022, direvisi: 19/07/2022, diterima: 20/07/2022

Abstract

This study aims to determine the crime of theft of customer data in the banking sector as a cyber crime. This study discusses the modus operandi that is often used in criminal acts of theft of customer personal data by cyber crime, legal arrangements to resolve these problems and also countermeasures that can be taken to prevent these crimes. This research is a normative legal research that is perspective using primary and secondary legal materials which are analyzed using deductive logic reasoning method. The technique of collecting legal materials used is literature study. The results of this study indicate that the development of information and communication technology in Indonesia has led to the development of new crimes that can be done virtually, namely cyber crime. Cyber crime that occurs in the banking sector is a case of personal data theft which in this study uses an approach to the regulation of the ITE Law, the Criminal Code and the Banking Law. Banking crimes in this study can be prevented using 2 (two) ways, namely penal policy and non-penal policy.

Keywords : *Cyber Crime*, *thesft*, *banking sector*

Abstrak

Penelitian ini bertujuan untuk mengetahui mengenai Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai *Cyber Crime*. Penelitian ini membahas mengenai modus operandi yang sering digunakan dalam tindak pidana pencurian data pribadi nasabah secara *cyber crime*, pengaturan hukum untuk menyelesaikan permasalahan tersebut dan juga penanggulangan yang dapat dilakukan untuk mencegah tindak pidana tersebut. Penelitian ini merupakan penelitian hukum normatif yang bersifat perspektif dengan menggunakan bahan hukum primer maupun sekunder yang dianalisis dengan metode penalaran logika deduktif. Teknik pengumpulan bahan hukum yang digunakan adalah studi kepustakaanHasil penelitian ini menunjukan bahwa perkembangan teknologi informasi dan komunikasi di Indonesia menyebabkan adanya perkembangan kejahatan baru pula yang dapat dilakukan secara virtual

yaitu *cyber crime*. *Cyber crime* yang terjadi di bidang perbankan ini adalah kasus pencurian data pribadi yang mana dalam penelitian ini menggunakan pendekatan pengaturan UU ITE,KUHP dan juga UU Perbankan. Kejahatan tindak pidana perbankan dalam penelitian ini dapat dicegah menggunakan 2 (dua) cara yaitu secara *penal policy* dan *non penal policy*.

Kata Kunci : *Cyber Crime*, Pencurian, Bidang Perbankan

A. Pendahuluan

Perbankan sebagai salah satu sektor esensial dalam kehidupan bermasyarakat, memiliki kewenangan dalam pertukaran uang dan transaksi keuangan. Posisi ini sekaligus menempatkan perbankan sebagai salah satu sektor yang rawan terhadap adanya penyalahgunaan wewenang dalam perputaran uang maupun ketentuan - ketentuan perbankan baik dari pihak bank itu sendiri maupun dari pihak luar yang memanfaatkan sektor perbankan sebagai tempat untuk menyimpan hasil kejahatan. Dalam aktivitas perbankan ditemukan beberapa kegiatan dengan tujuan tertentu dan dipaksakan sehingga melewati atau melanggar ketentuan yang resmi, yang sering disebut tindak pidana perbankan. Tindak pidana perbankan dalam berbagai aktivitas perbankan tersebut berkaitan erat dengan sistem keamanan nya.[1]

Layanan perbankan saat ini berkembang bergitu cepat dengan tujuan untuk memudahkan akses layanan terhadap nasabah. Dalam upaya meningkatkan pelayanan tersebut perbankan tentunya menerapkan kemajuan teknologi yang saat ini sedang berkembang pesat salah satunya nya terdapa dalam Anjungan Tunai Mandiri (ATM) yang saat ini digunakan sebagai pengganti fungsi kasir yang dulunya dilakukan secara konvensional. ATM ini memberikan pelayanan

[1] Nida Rafa Arofah, Y. P. (2020). INTERNET BANKING DAN CYBER CRIME : SEBUAH STUDI KASUS DI PERBANKAN NASIONAL . *Jurnal Pendidikan Akuntansi Indonesia*:107

seperti penarikan Tunai dan beberapa fungsi kasir lainnya.[2]. Pada dasarnya kegiatan perbankan saat ini telah mengalami keperubahan yang lebih baik dan mudah diakses, secara umum kegitan perbankan yang telah mengadopi penggunaan teknologi dapat disebut dengan *electronical banking (E- Banking).*

Munculnya Perbankan elektronik ini merupakan suatu trobosan baru di bidang perbankan. Penikmat layanan E-Banking ini juga cukup banyak hal ini didorong juga karena pengguna internet di Indonesia cukup meningkat, menurut kominfo sepanjang 2021 pengguna internet di Indonesia meningkat 11 persen dari tahun sebelumnya, yaitu dari 175,4 juta menjadi 202,6 juta pengguna. [3]). Situasi pandemi juga meningkatkan penggunaan produk perbanakan yang diakses secara digital, hal ini karena kan produk perbankan secara online seperti pembayaran secara elektronik dinilai dapat mengurangi penyebaran virus dari mata uang.

Keunggulan yang ditawarkan olehe *E-Banking* tentunya juga memiliki potensi masalah besar yang ditimbulkan, Pemanfaatan layanan perbankan, khususnya transaksi elektronik perbankan ini menjadi titik mula terjadinya *cyber crime.* Kejahatan siber merupakan salah satu pula jenis kejahatan yang berkembang dikarenakan kemajuan teknologi yang terjadii saat ini. Kejahatan siber di bidang berbankan pada dasarnya memiliki tuuan yang sama dengan kejahatan di bidang perbankan yang dilakukan secara konvensional yaitu untuk mendapatkan informasi rekening, kartu kredit, serta meretas sistem basis data bank serta merampok bank.[4] (ALMAJED, 2015, p. 3). Dalam kejahatan siber terdapat dua tipe kejahatan. Tipe yang pertama adalah kejahatan di mana

[2] Sudarso, H. d. (2015). Penentuan Potensi Lokasi Atm Bni Menggunakan Analytical Hierarchy Process (Ahp) Dan Sistem Informasi Geografis (Studi Kasus: Kecamatan Tembalang). *Jurnal Geodesi Undip*, 25-32.

[3] (Agustini 2021 https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/

[4] ALMAJED, N. M. (2015). Prevention of crime in B2C ECommerce: How E-Retailers/Banks protect themselves from Criminal Activities. *Security and Safety.*

komputer menjadi target aktivitas kriminal, sedangkan Tipe yang kedua adalah kejahatan yang menggunakan komputer sebagai alatnya.

Cyber crime di bidang berbankan merupakan ancaman yang cukup berpotensi menyebabkan kerugian baik bagi pihak bank maupun nasabah. Data pribadi merupakan salah satu sasaran kejahatan siber ini, data pribadi nasabah dalam kegiatan perbankan merupakan suatu hal penting untuk menikmati layanan perbankan. Pencurian data pribadi yang sering terjadi di bidang perbankan dilakukan untuk mengakses layanan perbankan korban yang nantinya digunakan untuk memeras/merampok saldo nasabah itu sendiri. Pada awal tahun 2018 terjadi tindak kejahatan pencurian informasi kartu debit dengan menggunakan metode skimming yang terjadi pada 64 bank yang tersebar di seluruh dunia dan 13 diantaranya bank swasta dan pemerintah Indonesia. Kejadian tersebut mengakibatkan bank yang terdampak harus mengembalikan dana nasabah mencapai 18 Miliar. Hal tersebut mengindikasikan pentingnya penanganan yang cepat untuk mengatasi permasalahan-permasalahan tersebut di masa yang akan datang.

Data pribadi nasabah menjadi suatu hal yang penting dan harus dilindungi berdasarkan prinsip kerahasian perbankan. Untuk mendapatkan akses layanan transaksi elektronik, nasabah wajib mengisikan data diri. Data yang diisikan nasabah merupakan hak pribadi *(privacy right)* yang harus dijamin perlindungannya. Data nasabah seperti nama, tanggal lahir, nama ibu kandung, alamat rumah, alamat email, ataupun nomor handphone (HP) wajib dirahasiakan. Data diri nasabah ini seharusnya mendapatkan jaminan bebas dari gangguan siapapun, sebagaimana ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 26 ayat (1) yang menjelaskan bahwa kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Namun yang terjadi, data diri ini belum sepenuhnya mendapatkan perlindungan dari sistem keamanan perbankan.

Di Indonesia sendiri pengaturan mengenai pencurian data pribadi di bidang perbankan yang dilakukan secara *cyber* tersirat dan atur dalam beberapa undang undang yang mana undang undang yang paling dominan mengatur kejahatan ini adalah Undang Undang Nomor 19 Tahun 2016 tentang Perubahan Undang Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Namun Undang Undang ini terkadang masih membutuhkan rujukan pengaturan lain karena bersifat sangat umum seperti halnya apabila terdapat permasalahan di bidang perbankan dan pencurian data pribadi maka akan merujuk pengaturan lain yang sesuai dengan bidang tersebut. Kurang komperhensifnya cyber law yang ada di Indonesia ini tentunya mendatangkan tantangan tersendiri dalam menyelesaikan kasus kasus cyber crime di Indonesia.

Berdasarkan latar belakang yang telah dipaparkan diatas penelitian ini akan memberikan kajian mengenai Bagaimana modus operandi, Pengaturan dan juga pencegaha tindak pidana pencuriaan data nasabah dalam bidang perbankan yang dilakukan secara *cyber crime*. Metodelogi Penelitian dalam jurnal ini adalah dengan Jenis penelitian hukum normatif atau sering disebut sebagai penelitian hukum doktrinal. Sifat penelitian yang digunakan dalam penelitian ini adalah bersifat preskriptif dan terapan. Preskriptif adalah mempelajari tujuan hukum, nilai-nilai keadilan, validasi aturan hukum, konsep hukum, dan norma hukum. Penelitian preskriptif bertujuan untuk memberikan gambaran atau merumuskan masalahsesuai dengan keadaan atau fakta yang ada. Pendekatan yang digunakan penulis dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*), pendekatan kasus (*case approach*) dan pendekatan konseptual (*conceptual approach*). Sumber bahan hukum yang penulis gunakan yaitu bahan hukum primer berupa Undang-Undang Nomor 19 Tahun 2016 perubahan atas UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor Undang-undang Nomor 10 Tahun 1998 tentang Perbankan,Undang Undang Nomor 3 Tahun 2011 Tentang Transfer Dana ,Undang – Undang Nomor 21 tahun 2011 tentang OJK, Kitab

Undang Undang Hukum Pidana Bahan hukum sekunder berupa hasil penelitian, tulisan-tulisan karya ilmiah, jurnal, kamuskamus hukum, dan hasil wawancara yang secara tidak langsung memberikan keterangan terkait bahan hukum primer dan mampu mendukung penelitian ini.

Metode pengumpulan data yang digunakan penulis dalam penelitian ini adalah studi kepustakaan *(library research*). Pengumpulan data yang dilakukan menggunakan cara menganalisis suatu konten yang berkaitan. Teknik ini digunakan untuk mendapatkan landasan teori dengan mengkaji dan 6 mempelajari buku, peraturan perundang-undangan, dokumen, arsip, laporan, dan hasil penelitian yang serupa atau saling berkaitan dengan masalah yang diteliti.[5]

B. Pembahasan

B.1.Modus operandi tindak pidana pencuriaan data nasabah dalam bidang perbankan secara *cyber crime*.

Masyarakat selalu bergerak dan tumbuh kearah yang lebih modern, begitu juga hukum, hukum dan masyarakat merupakan suatu hal yang tidak dapat dipisahkan satu sama lain. Hukum harus berkembang sejalan dengan kondisi masyarakat diwilayah tersebut agar hukum tetap dapat menjalankan perannya sebagai pengatur kehidupan. Perkembangan teknologi yang terjadi di masyarakat saat ini tentunya akan mempengaruhi tipologi kejahatan yang kian berubah pula. Seperti halnya perkembangan teknologi menyebabkan pengguna internet di Indonesia sendiri semakin naik dan tentunya kejahatan yang dilakukan secara virtual pun saat ini kian perkembang pesat. *Cyber crime* di ruang virtual seolah tidak bisa terelakkan lagi seiring dengan kemajuan teknologi yang secara nyata telah menghadirkan dunia tanpa batas *(borderless). Cyber crime* menjadi sisi negatif dari perkembangan internet dan teknologi yang semakin pesat. Kejahatan di ruang siber ini pun telah berhasil menerobos dunia

[5] Pieter Mahmud Marzuki. 2014. Penelitian Hukum (Edisi Revisi). Jakarta: PT. Raja Grafindo Persada:273

perbankan. Sistem keamanan perbankan saat ini masih terus menghadapi kejahatan yang berkaitan dengan pelanggaran dan penyalahgunaan perkembangan teknologi tinggi *(hi tect)* yang mutlak harus digunakan dalam perbankan. Kejahatan dalam pemanfaatan teknologi ini yang menyelinap di balik semakin besarnya peran internet dalam sebagian berbesar sektor kehidupan. *Cyber crime* menjadikan teknologi informasi sebagai media untuk perbuatan melawan hukum.

Cyber crime telah berkembang begitu pesat di segala lini kehidupan manusia, salah satu bidang yang rentan terkena kejahatan siber adalah bidang perbankan, kejahatan dibidang perbankan yang sebelumnya dilakukan secara konvensial kini dapat dilakukan secara virtual. Dalam kejahatan siber terdapat dua tipe kejahatan, tipe pertama adalah kejahatan yang menjadikan komputer menjadi target aktivitas kriminalnya dan tipe yang kedua adalah kejahatan yang menggunakan komputer sebagai alatnya (Faridi 2018:58). Sebelum membahas secara lebih detail mengenai modus operandi dalam pencurian data pribadi di bidang perbankan perlu diketahui bahwa secara terminologi tindak pidana perbanakan memiliki makna yang berbeda dengan tindak pidana di bidang perbankan. Tindak pidana perbankan merupakan tindak pidana yang ada dalam Undang-Undang Nomor 7 Tahun 1992 sebagaimana telah diubah dengan Undang-undang No.10 Tahun 1998 tentang Perbankan. Sedangkan tindak pidana dibidang perbankana merupakan suatu tindakan yang dilarang dan melibatkan bank dalam kegiatannya.

Terdapat beberapa bentuk *cyber crime* yang sering terjadi pada sektor jasa perbanakan antara lain adalah sebagai berikut

a. *Typo Site*

   Typo site, yaitu membuat nama domain dan alamat situs yang mirip dengan situs resmi. Pelaku memanfaatkan kekeliruan dari pengguna internet dalam pengetikan alamat situs yang dicari.

b. *Keylogger/ keystroke recorder.*

Kegiatan ini dilakukan dengan menggunakan software atau program keylogger. Cara kerja dari keylogger adalah dengan mencatat segala aktivitas yang dilakukan oleh pengguna internet melalui hurufhuruf yang diketikkan pada keyboard. Dalam berselancar di dunia maya, pengguna internet mungkin saja memasukkan nomor identitas dan password yang dapat dimanfaatkan oleh pelaku. Cara kejahatan ini biasanya terjadi pada tempat umum yang digunakan untuk mengakses internet seperti warnet atau restoran, bandara dan tempat umum lainnya yang menyediakan komputer didukung dengan fasilitas internet.

c. *Sniffing.*
   Sniffing cara yang digunakan oleh pelaku dengan mengamati paket data internet yang digunakan oleh pengguna untuk mendapatkan nomor identitas dan password yang bersangkutan
d. *Brute Force Attacking*
   yaitu upaya pencurian nomor identitas dan password melalui mencoba kemungkinan atas kombinasi yang dibuat.
e. *Web Deface: System Exploitation,*
   yaitu eksploitasi sistem dengan megganti tampilan awal dari sebuah situs resmi.
f. *Email Spamming,*
   yakni dengan mengirimkan email kepada pemilik akun dengan menawarkan produk-produk atau menyatakan bahwa pemilik akun telah memenangkan suatu undian.
g. *Denial of Service*, yaitu pelumpuhan sistem elektronik dengan membanjiri akun atau sistem elektronik dengan data dalam jumlah yang besar.
h. *Virus, worm, trojan:* Penyebaran virus komputer dilakukan untuk menyerang sistem komputer, memperoleh data, memanipulasi data atau tindakan lain yang dilakukan secara melawan hukum.

Bentuk bentuk cyber crime diatas merupakan suatu bentuk *cyber crime* yang terjadi di ranah perbanakan yang mana bentuk bentuk diatas akan diterapkan

dalam modus operandi tindak pidana pencurian data pribadi dibidang perbankan sebagi berikut.

a. *Skimming*

Skimming merupakan modus kejahatan di bidang perbankan bertujuan mencuri informasi dari kartu debit atau kredit milik nasabah, menggunakan alat khusus bernama Skimmer. 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. Pemasangan skimmer bertujuan untuk merekam data elektronik kartu ATM nasabah pada pita magnetic yangterdapat di kartu ATM. Sedangkan kamera tersembunyi bertujuan untuk mengetahui nomor PIN masing - masing nasabah. Setelah data tersebut diketahuikemudian dibuatkan kartu yang baruhasil duplikasi dari data-data tersebutdan pelaku dapat langsung menggunakankartu ATM palsu tersebut tanpasepengetahuan nasabah. [6]

b. *Carding*

Carding adalah tindakan mencuri kartu kredit dengan menggunakan kartu kredit dalam kegiatan perbankan. *Carding* biasanya dilakukan untuk mendapatkan data kartu kredit korban secara tidak sah (*illegal interception).* Kemudian setelah itu kartu kredit digunakan untuk berbelanja si toko online (*forgery).* Modus tersebut biasanya terjadi dikarenakan lemahnya sistem pengecekan yang dipakai dalam memastikan identitas pemesan barang di toko online. Kejahatan siber secara *carding* ini dapat terjadi karena dalam kasus carding ini terdapat 4 jenis

1) ***misuse of card data*** yang berupa penyalahgunaan kartu kredit yang tidak dipresentasikan, merupakan kejadian dimana pengguna kartu kredit tidak

[6] Judiawan, K. (2013). Perlindungan Hukum Terhadap Nasabah Korban Kejahatan Penggandaan Kartu ATM pada Bank Swasta di Denpasar. *Jurnal Magister Hukum Universitas Udayana:* 4

menyadari kartunya sudah digunakan oleh pihak lain sampai ia menerima tagihan tersebut.

2) ***Wiretapping*** dilakukan dengan cara menyadap transaksi kartu kredit melalui jaringan komunikasi. Kejahatan ini bisa mengakibatkan kerugian yang besar bagi korbannya.
3) ***Counterfeiting*** jenis kejahatan dengan modus pemalsuan kartu kredit. Biasanya mereka menggunakan kartu palsu yang dibuat sedemikian mirip dengan kartu asli. Carding jenis ini biasanya dilakukan oleh perorangan hingga sindikat pemalsu kartu kredit yang memiliki keahlian tertentu.

c. *Phising*

Penipuan *Phising* yang merupakan salah satu bentuk *cyber crime* biasanya dilakukan melalui pesan e-mail penipuan dari perusahaan yang sah (misalnya, universitas, penyedia layanan internet, bank). Pesan dalam email ini biasaya mengarahkan seseorang kesitus web palsu atau membuat seseorang untuk membocorkan informasi pribadi (misalnya, pasword, kartu kredit, atau update akun lainnya). Para pelaku kemudian meggunakan informasi pribadi untuk melakukan pencurian identitas. Identitas tersebut kemudian digunakan unutuk kejahatan yang merugikan pemilik. Kejahatan ini biasa terjadi pada pengguna online banking. [7](Widodo, 2013 :88)

Pishing dapat juga dioperasikan dengan cara mengirimkan e-mail atau membuat suatu wesite yang seakan-akan sebagai penyelenggara e-commerce, sehingga banyak pengguna internet yang memasukkan data atau online ke alamat yang diperkenalkan tersebut. Secara phising dilakukan dengan mendistribusikan e-mail yang berisi pesan tentang alamat pengirim, mekanisme kerja, dan nama suatu perusahaan sehingga seakan-akan tampak menunjukkan identitas bank, atau perusahaan asuransi, atau perusahaan pengelola kartu kredit, atau lembaga keuangan lain. Pesan palsu dalam e-mail tersebut dirancang secara meyakinkan untuk mengelabuhi penerima pesan,

[7] Widodo. 2013. *Memerangi Cybercrime Karateristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi.* Yogjakarta: Asswaja Pressindo:88

dengan cara membuat pengumuman data tentang identitas perusahan palsu yang meliputi rekening, penanggungjawab, kartu kredit, jaminan sosial, dan lain-lain. Bahkan seringkali dalam e-mail tersebut disertakan foto pejabat palsu dan sejumlah data perusahaan palsu. Jika ada penerima e-mail tertarik dengan isi pesan tersebut, maka akan melakukan transaksi melalui internet sehingga data korban dan PIN dapat direkam oleh pelaku phising. Perbuatan ini merugikan banyak orang, karena akan dapat menyebabkan penipuan uang, pencurian identitas, dan aktivitas curang lainnya melalui internet. [8]

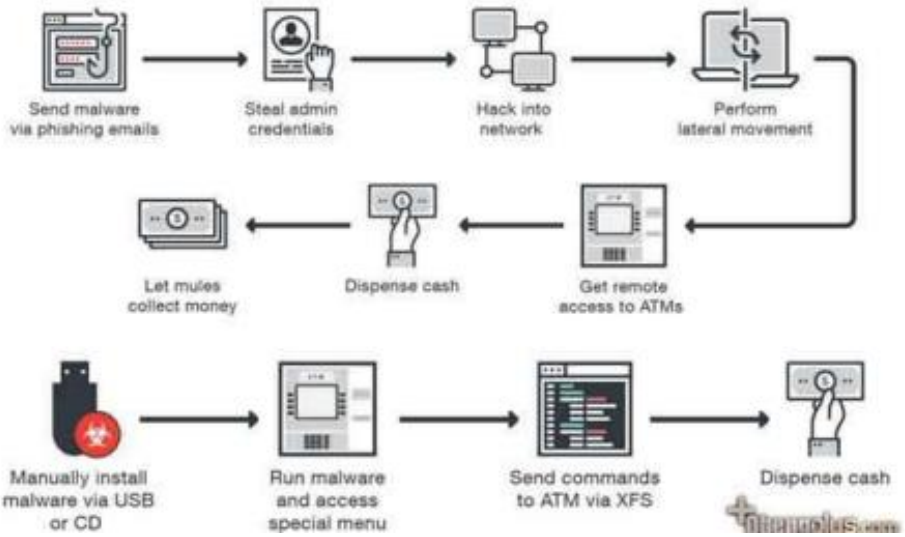
Dalam dunia perbankan phising merupakan salah satu modus operandi tindak pidana pencurian data pribadi nasabah secara *Cyber Crime* yang mengakibatkan *Fraud*. *Fraud* berarti tindakan melanggar hukum yang dilakukan seseorang atau sekelompok orang untuk mendapatkan keuntungan finansial dari penggunaan kartu kredit yang bukan menjadi hak miliknya. Fraud biasanya dapat menyerang kartu kredit dan online banking. Dalam kasus fraud dalam kartu kredit ini phishing biasanya mengincar 4 digit nomor di belakang kartu kredit, dan nomor PIN-nya. Informasi ini kemudian digunakan oleh pelaku untuk bertransaksi atas nama nasabah.

d. *Malwere*

Malware merupakan singkatan dari malicious software yang artinya software yang tidak diinginkan dalam sistem komputer, biasanya malware dibuat untuk mencuri data informasi yang bahkan dapat merusak sebuah sistem computer.[9] Berikut adalah ilustrasi bagaimana alur bagaimana suatu malware dapat menyerang sistem komputer

[8] Ibid.89

[9] Kurniawan, & Prayudi. (2014). Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics. *HADFEX (Hacking and Digital Forensics*:1-5



Terdapat dua jalur yang menjadi awal sebuah sistem komputer terserang oleh malware yaitu dapat melalui USB drive dan melalui jaringan internet. stem Komputer yang terinfeksi malware melalui USB Drive biasanya tidak memiliki pengaman seperti antivirus atau sejenisnya sehingga malware yang sudah terinstall di USB dapat dengan mudah masuk ke sistem komputer. Selanjutnya sistem komputer yang terinfeksi melalui jaringan internet yaitu ketika pengguna membuka email atau website. Pada email yang berbahaya biasanya akan langsung disaring ke spam oleh sistem namun tidak banyak dari email tersebut juga masuk ke inbox. Malware ini akan berjalan ketika objek yang terinfeksi di dalam email itu di klik dan selanjutnya ketika sistem komputer yang sudah terinfeksi malware maka informasi pribadi termasuk data-data perbankan yang tersimpan di komputer.

Malware ini dapat menyerang nasabah yang menikmati layanan perbankan seperti layanan internet banking yang mengintegrasikan email serta data pribadi lainnya dalam menikmati layanan perbankan ini

e. *Hacking*

Merupakan 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. Contohnya, aksi hacking yang kerap terjadi adalah pembobolan kata sandi. rangan hacking yang mungkin terjadi pada transaksi pada perbankan seperti *Distributed Denial of service* (DDOS). DDOS merupakan salah satu serangan yang sering dilakukan pada sistem server baik pada perusahaan maupun perbankan. Untuk dapat melakukan peretasan, hacker akan melakukan scan port yang terbuka kemudian mulai malukan menyerang pada jaringan bank.

Dari berapa modus operandi diatas menunjukan bahwasanya kejahatan di bidang perbankana mengalami perubahan sesuai dengan perkembangan zaman dan teknologi, yang semula kejahatan hanya dilakukan secara langsung dan nyata saat ini kejahatan dapat dilakukan di ruang virtual yang tidak mengenal batas dan waktu. Tentunnya hal ini mendorong agar sistem pengaturan hukum berkembang sesuai dengan perkemvbangan zaman

B.2 Pengaturan mengenai tindak pidana pencurian data nasabah di bidang perbankan secara *cyber crime*

Penelitian ini membahas pengaturan mengai pencurian data pribadi nasabah yang dilakukan secara *cyber crime* dilihat dari beberapa prespektif pengaturan yang ada di Indonesia. Untuk mempersempit bahasan dan memfokuskan penelitian ini maka dalam penelitian ini akan membahas pengaturan mengenai tindak pidana pencurian data pribadi ini ditinjau dari KUHP, UU ITE dan UU Perbanka.

a. **Pengaturan mengenai tindak pidana pencurian data nasabah di bidang perbankan secara *cyber crime* dalam prespektif KUHP**

Ketentuan dalam KUHP yang dapat digunakan untuk mengadili *cyber crime* dengan cara melakukan penafsiran extensif adalah ketentuan tentang tindak pidana pemalsuan (sebagaimana diatur dalam Pasal 263 sampai dengan Pasal 276), tindak pidana pencurian (sebagaimana diatur dalam Pasal 362 sampai dengan 367), tindak pidana penipuan (bagaimana diatur dalam Pasal 378 sampai dengan Pasal 395), dan tindak pidana perusakan barang (sebagaimana diatur dalam Pasal 407 sampai dengan Pasal 412). Mengenai pencurian data

pribadi nasabah di bidang perbankan sendiri dapat diterapkan pula pada pasal dalam KUHP ini seperti salah satunya adalah phising. Pencurian data nasabah menggunakan teknik phising dilakuan pelaku dengan cara mengelabuhi nasabah dengan mengirimkan email palsu yang berisi, bahwa nasabah diwajibkan untuk meng upgrade internet Bankking milik mereka, jika tidak segera meng upgrade maka internet Bankking milik nasabah akan diblokir. Tidak hanya perintah untuk segera meng upgrade *internet Banking* milik nasabah saja, tetapi didalam email tersebut nasabah diarahkan pelaku untuk masuk kedalam website Bank tersebut. Website tersebut merupakan Website palsu yang dibuat sama persis menyerupai Website asli milik Bank, sehingga nasabah merasa yakin bahwa Website tersebut benar Website asli milik Bank yang dimaksud. Ketika nasabah sudah yakin dengan Website tersebut, nasabah meng upgrade internet Bankking milik mereka dengan memasukkan Password dan Username. Tanpa disadari nasabah bahwa ketika nasabah memasukkan Password dan Username milik mereka pada saat itu juga pelaku mengetahui Password dan Username milik nasabah. Setelah pelaku mendapatkan Password dan Username milik nasabah pelaku menggunakan Password dan Username tersebut untuk masuk kedalam internet Bankking milik nasabah yang kemudian pelaku dengan leluasa menggunakana internet Bankking tersebut dan mentransfer sejumlah uang yang milik nasabah yang berada di rekening milik nasabah ke rekening pelaku.

Kejadian seperti diatas ini dapat di kenai pasal 378 KUHP, yang berbunyi Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutanng mapun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun.

b. **Pengaturan mengenai tindak pidana pencurian data nasabah di bidang perbankan secara *cyber crime* dalam prespektif UU perbanakan**

Perlindungan data pribadi nasabah di bidang perbankan dilakukan oleh bank berdasarkan prinsip kerahasian *(confidential Principle)*. Undang Undang Nomor 10 tahun 1998 telah mengatur mengenai prinsip kerahasiaan ini yang mana secara jelas bahwa bank diwajibkan untuk melindungi data pribadi nasabahnya, hal ini berarti bank harus merahasiakan segala hal yang berhubungan dengan data dan informasi nasabah, baik dengan keadaan keuanganya maupun informasi yang bersifat pribadi. (Ghazali, 2010: 30) Dalam Undang Undang perbankan Pengaturan mengenai kerahasian bank ini diatur dalam Pasal 1 ayat (28) Undang –Undang Perbanakan menjelaskan bahwa rahasia bank ditafsirkan sebagai segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya.

Secara lebih rigid perlindunga data pribadi nasabah perbankan diatur dalam Pasal 40 ayat (1) UU Perbankan menegaskan bahwa "Bank Wajib merahasiakan keterangan nasabah penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44 dan Pasal 44A". Berdasarkan bunyi Pasal tersebut dapat menujukkan bahwa Bank memiliki sifat kerahasiaan yang sangat ketat. Dimana pihak bank dilarang untuk melakukan pembukaan atau penyebaran data-data nasabah dikarenakan hal tersebut dinilai sebagai rahasia bank. Sehingga apabila terjadinya kebocoran data nasabah baik penyimpan maupun pinjaman, maka pihak Bank tersebut dapat diancam melakukan pelanggaran atas Pasal 47 ayat (2) UU Perbankan yang menerangkan bahwa"Anggota Dewan Komisaris, Direksi, pegawai bank atau Pihak Terafiliasi lainnya yang sengaja memberikan keterangan yang wajib dirahasiakan menurut Pasal 40, diancam dengan Pidana penjara sekurang-kurangnya 2 (dua) tahun serta denda sekurang-kurangnya Rp. 4.000.000.000,- (empat miliar rupiah) dan paling banyak Rp. 8.000.000.000,- (delapan miliar rupiah)".

c. **Pengaturan mengenai tindak pidana pencurian data nasabah di bidang perbankan secara *cyber crime* dalam prespektif UU ITE**

Dalam tindak pidana pencurian data pribadi nasabah tentunya objek data pribadi nasabah merupakan hal yang cukup penting. Di Indonesia pengaturan mengenai Data Pribadi diatur secara Implisit dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kejahatan terhadap privasi atau data pribadi oleh UU ITE.Penerapan sanski hukum terhadap pelaku pencurian data pribadi nasabah terdapat pada pasal 30 , Pasal 32 dan pasal 35. Selain itu untuk ketentuan pidana terdapat pada pasal 46, Pasal 48, Pasal 49, Pasal 51 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kejahatan terhadap privasi atau data pribadi oleh UU ITE dapat dijelaskan mengenai penerapan sanksi pencurian adalah sebagai berikut Setiap Setiap perbuatan melawan hukum dengan mengakses sistem elektronik yang bertujuan untuk memperoleh Informasi/Dokumen Elektronik dengan cara melanggar sistem pengamanan dianggap sebagai tindak pidana sesuai Pasal 46 jo Pasal 30 UU ITE. Perbuatan ini diancam dengan sanksi pidana penjara paling lama 6 sampai 8 tahun dan/atau denda paling banyak Rp600.000.000,00 sampai Rp800.000.000,00.

B.3 Pencegahan Pencurian Data Nasabah Dalam Bidang Perbankan Yang Dilakukan Secara *Cyber Crime*

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*). Kebijakan Hukum Pidana (*Penal Policy*) atau Kebijakan Kriminal (*Crimnal Policy*) adalah suatu upaya yang rasional dari lembaga kenegaraan yang punya kompetensi untuk menanggulangi kejahatan Ini berarti kebijakan hukum pidana (*Penal Policy*) merupakan proses penegakan hukum pidana secara menyeluruh dan total. Ketiga tahapan formulasi, aplikasi dan eksekusi merupakan satu kesatuan jalinan mata rantai yang bulat sehingga proses fungsionalisasi/operasionalisasi penegakan hukum pidana dapat mewujudkan kebijakan sosial (*Social Policy*), yang melahirkan kesejahteraan

sosial dan perlindungan kepada masyarakat. Sedangkan *non penal police* merupakan suatu pencegahan hokum pidana yang dilakukan diluar pengadilan.

Dalam tindak pidana pencurian data pribadi di bidang perbankan ini telah dilakukan beberapa kebijakan penal policy yang dilaksanakan seperti dengan adanya Undang Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, Undang – Undang 21 tahun 2008 tentang perbankan syariah, Undang- Undang Nomor 24 Tahun 2004 Tentang lembaga penjamin simpanan. Diharapkan Kebijakan pidana tersebut dapat memberika efek jera bagi pelaku dan tidak menimbulkan pengulangan kejahatan bagi pelaku yang lain

Secara *non penal* merupakan suatu pencegahan yang dilakukan diluar jalur pidana, berikut adalah beberapa hal yang dilakukan sebagai pencegahan secara non penal

a. Kerjasama Internasionall, menilik dari sifat *cyber crime* yang transnasional maka diperlukan kerjasama internasional yang intensif baik dalam penegakan hukum pidana dalam penegakan hukum pidana maupun dalam bidang teknologi berupa pembentukan jaringan informasi yang kuat, misalnya program "*24 hours point cantact*" untuk menghadapi kejahatan cybercrime. Pelatihan personil penegak hukum yang memadai, harmonisasi hukum dan penyebarluasan kesepakatan-kesepakatan internasional
b. Rencana Aksi Nasional (*National Action Plan*) di Indonesia Pemerintah dan beberapa komunitas teknologi informasi nsional perlu menggalang kerjasama guna menanggulangi kejahatan di dunia maya (*Cyber Crime)* Kegiatan yang sudah dilakukan tersebut misalnya melalui pendirian Indonesia *Forum on Inromation for Infocom Incident Respomse adn Security Team* (ID FIRST), yang diharapkan menciptkan sinergi antara pemerintah, kepolisian, dan industri teknologi informasi dalam mencegah dan memberantas kejahatan dunia maya melalui internet

C. Penutup

C.1. Kesimpulan

Sesuai dengan perkembangan teknologi yang mempengaruhi perkembangan masyarakat pula maka kejahatan yang ada disekitar masyarakat berkembang pula begitu juga dibidang perbankan seperti modus operandi tindak pidana dibidang perbankan. Tindak Pidana dibidang perbankan yang sebelumnya dilakukan secara konvensional tanpa menggunakan komputer saat ini *cyber crime* menjadi tantangan yang cukup besar khusunya dalam pencurian data pribadi nasabah, mudahnya akses internet membuat kreativitas masyarakat dalam melakukan kejahatan juga berkembang pesat, terdapat beberapa modus operandi dalam pencurian data pribadi nasabah yang dilakukan secara cyber crime yang sering terjaadi di sektor perbanakan yaitu ***Skimming*** merupakan modus kejahatan di bidang perbankan bertujuan mencuri informasi dari kartu debit atau kredit milik nasabah, menggunakan alat khusus bernama Skimmer, ***carding***adalah tindakan mencuri kartu kredit dengan menggunakan kartu kredit dalam kegiatan perbankan. *Carding* biasanya dilakukan untuk mendapatkan data kartu kredit korban secara tidak sah (*illegal interception).* Kemudian setelah itu kartu kredit digunakan untuk berbelanja si toko online (*forgery)*, ***Phising*** yang merupakan salah satu bentuk *cyber crime* biasanya dilakukan melalui pesan e-mail penipuan dari perusahaan yang sah (misalnya, universitas, penyedia layanan internet, bank). Pesan dalam email ini biasaya mengarahkan seseorang kesitus web palsu atau membuat seseorang untuk membocorkan informasi pribadi (misalnya, pasword, kartu kredit, atau update akun lainnya), ***Malware*** merupakan singkatan dari malicious software yang artinya software yang tidak diinginkan dalam sistem komputer, biasanya malware dibuat untuk mencuri data informasi yang bahkan dapat merusak sebuah sistem komputer dan yang terakhir adalah ***hacking*** Merupakan istilah kejahatan siber yang cukup umum. Aksi ini dilakukan dengan cara mengakses sistem komputer korban tanpa hak

Mengenai pengaturan *cyber crime* di Indonesia tidak diatur secara rinci dalam suatu pengaturan perundang-undangan. Pengaturan yang secara eksplisit terlibat sangat kental dengan kejahatan cyber di Indonesia saat ini adalah UU ITE, jika di korelasikan dengan pencurian data pribadi dibidang perbankan tentunya undang undang perbankan dan KUHP sebagai induk hukum pidana di Indonesia akan tetap dijadikan rujukan dalam menyelesaikan persoalan mengenai pencurian data pribadi dibidang perbanakan yang dilakukan secara *cyber crime*. Dalam penyelesaian tindak pidana cyber crime di Indonesia modus operadi yang digunakan didasarkan pada pengenaan pasal di UU ITE namun selama proses pengadilanya tidak mengabaikan pula ketentuan ketentuan dalam pengaturan lain yang sesuai dengan tindak pidana yang dilakukan

Terdapat dua langkah pencegahan dalam dalam mencegah tindak pidana pencurian data pribadi di bidang perbanakan ini yaitu yang pertama adalah secara penal policy yaitu pencegahan dengan penerapan hukum pidana atau secara peradilan di Indonesia penerapan ini sudah ada pada ketentuan pidana dalam beberapa pengaturan seperti dalam UU ITE, UU Perbanakan dan regulasi lain yang mengatur tentang pencurian data pribadi dan kejahatan di bidang perbanakan. Kedua adalah pencegahan secara non penal policy atau pencegahan yang dilakukan tanpa dengan menggunakan ketentuan pidana seperti halnya memperbaiki sistem keamanan dalam dunia perbankan agar terhidar dari tindakan pencurian data pribadi, meningkatkan kinerja pemerintah, kepolisian, dan industri teknologi informasi dalam mencegah dan memberantas kejahatan dunia maya melalui internet, meningkatkan kesadaran nasabah akan pentingnya perlindungan akun dan penikatan keamana cyber dalam melakukan transaksi keuangan.

C.2. Saran

Dalam menghadapi tantangan teknologi yang semakin maju maka dalam bidang hukum diperlukan suatu pembaharuan regulasi yang dapat mengakomodi jalanya kehidupan masyarakat oleh karena itu penulis

mengharapkan kepada lembaga pembentuk undang undang yang tentunya didalamnya melibatkan ahli pidana dan cyber crime dalam pembentukan regulasinya segera membentuk pengaturan mengenai cyber crime yang masif,komperhensif dan sesuai dengan pribadi bangsa Indonesia agar tercipta penegakan hukum khususnya pencurian data pribadi di bidang perbankan dengan teknik cyber crime ini

Perbanakan sebagai lembaga vital yang memiliki tugas menghimpun dan menyalurkan dana masyarakat sudah seharusnya meningkatkan kembali sistem keamanan komputer agar tidak mudah terserang kejahatan siber yang semakin berkembang pesat modus operandinya, karena mengingat data pribadi wajib dijaga oleh perbankan berdasarkan asas kerahasian.

Daftar Pustaka

Arief, B. N. 2007. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam .* Jakarta: Kencana Perdana Media Group**.**

ALMAJED, N. M. (2015). Prevention of crime in B2C ECommerce: How E-Retailers/Banks protect themselves from Criminal Activities. *Security and Safety.*

Faridi, M. K. (2018). Kejahatan Siber dalam Bidang Perbankan . *CyberSecurity dan Forensik digital* , 56-61.

Judiawan, K. (2013). Perlindungan Hukum Terhadap Nasabah Korban Kejahatan Penggandaan Kartu ATM pada Bank Swasta di Denpasar . *Jurnal Magister Hukum Universitas Udayana* , 4.

Maskun. 2013. *Kejahatan Siber (Cyber Crime).* Jakarta: Kencana Pieter Mahmud Marzuki. 2014. Penelitian Hukum (Edisi Revisi). Jakarta: PT. Raja Grafindo Persada

Kurniawan, & Prayudi. (2014). Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics. *HADFEX (Hacking and Digital Forensics*, 1-5.

Riswadi, B. A. 2006. *Hukum Cyberspace.* Yogjakarta: Gitanagari

S, I. (2014). systematic literature review: Security challenges of mobile banking and payment System . *International Journal of u-and e-Service, Science and Technology,*, 107-116.

Sudarso, H. d. (2015). Penentuan Potensi Lokasi Atm Bni Menggunakan Analytical Hierarchy Process (Ahp) Dan Sistem Informasi Geografis (Studi Kasus: Kecamatan Tembalang). *Jurnal Geodesi Undip*, 25-32.

Widodo. 2013. *Memerangi Cybercrime Karateristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi.* Yogjakarta: Asswaja Pressindo