# DATA LEAKAGE OF BANKING CUSTOMERS IN THE PERSPECTIVE OF CRIMINAL LAW

**(Analysis of Bank BSI Customer Data Leakage Cases)**

# KEBOCORAN DATA NASABAH PERBANKAN DALAM PERSPEKTIF HUKUM PIDANA

# (Analisis Kasus Kebocoran Data Nasabah Bank BSI)

# Khabib Irfansyah

# Sekolah Tinggi Ilmu Hukum IBLAM, Jl. Kramat Raya No.25, RT.3/RW.2, Kramat, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10450

# Heri Qomaruddin

# Sekolah Tinggi Ilmu Hukum IBLAM, Jl. Kramat Raya No.25, RT.3/RW.2, Kramat, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10450

***Abstract***

*Crime in technology is always changing so that existing legal regulations cannot fully protect society. The advancement of the world of technology and the Internet not only has a positive impact that is useful for facilitating communication but has also led to rampant crime in that field. There are so many crime cases recorded through technology, the crime is called Cybercrime. One of the cases related to cybercrime is the theft of banking customer data, the latest being customers from Bank Syariah Indonesia (BSI). Recently, a number of Bank Syariah Indonesia or BSI customers have complained that they cannot access their respective BSI Mobile applications. According to the company, it is currently carrying out system maintenance so that BSI services cannot be accessed for a while. This type of research is normative juridical research. The nature of the research in this study is analytical descriptive in nature. The type of data used in this research is library research. The current banking security system continues to face crimes related to violations and misuse of high-tech developments (hi-tect) which absolutely must be used in banking. Crime in the use of this technology that sneaks behind the increasing role of the internet in most sectors of life. Cyber crime makes information technology a medium for unlawful acts. Cybercrime has developed so rapidly in all lines of human life, one area that is vulnerable to cybercrime is the banking sector, crimes in the banking sector that were previously carried out conventionally can now be carried out virtually.*

***Keywords***: *Customers, Banking, Criminal Law*

**Abstrak**

Kejahatan dalam Teknologi selalu mengalami perubahan sehingga Regulasi regulasi hukum yang sudah ada belum dapat melindungi masyarakat sepenuhnya. Majunya dunia Teknologi dan Internet tidak hanya memberikan dampak positif yang berguna untuk mempermudah komunikasi namun juga menyebabkan maraknya kejahatan dalam bidang tersebut. Ada begitu banyak kasus kejahatan yang tercatat melalui teknologi,kejahatan itu dinamakan *Cybercrime.* salah satu kasus terkait *cybercrime* ialah Kasus pencurian data nasabah perbankan yang terbaru ialah nasabah dari Bank Syariah Indonesia (BSI). Beberapa terakhir ini, sejumlah nasabah Bank Syariah Indonesia atau BSI mengeluh tidak bisa mengakses aplikasi BSI Mobile mereka masing-masing. Menurut perusahaan, pihaknya tengah melakukan *maintenance system* sehingga membuat layanan BSI tidak bisa diakses untuk sementara waktu. Jenis penelitian yang dilakukan adalah penelitian yuridis normatif. Sifat penelitian dalam penelitian ini adalah bersifat deskriptif analitis. Jenis data yang digunakan dalam penelitian ini adalah penelitian kepustakaan (*library research*). 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.

**Kata Kunci**: Nasabah, Perbankan, Hukum Pidana

### PENDAHULUAN

Sebagai negara hukum, Indonesi Perkembangan teknologi sudah membuat batasbatas ruang dalam beberapa aspek di dunia menjadi tidak lagi terbatas. Artinya kontrol atau pengendalian menjadi semakin lemah apabila tidak diikuti dengan pekembangan hukum. dapat dikatakan bahwa teknologi informasi adalah bom waktu, meskipun tujuannya adalah untuk meningjatkan kesejahteraan serta kemajuan dari peradaban manusia, namun sewaktu- waktu dapat pula menjadi ancaman bagi manusia karena telah menjadi sarana perbuatan melawan hukum (Budi Suhariyanto, 2012).

Tujuan dan fungsi hukum adalah untuk menegakkan keadilan, memberi kepastian serta mencptakan kesejahteraan hidup bagi masyarakat. Sejak tahun 1998 atau pada era reformasi, mulai banyak diterbitkan peraturan perundang-undangan dengan menyesuaikan dinamika globalisasi. Peraturan perundang-undangan ini diharapkan bisa membawa masyarakat pada kondisi hidup yang jauh lebih baik dari keadaan sebelumnya. Menjadi titik awal dari berkembangnya hukum sebagai peraturan yang mengikuti perkembangan zaman, tentunya masa-masa tersebut terus diikuti dengan dikeluarkannya peraturan-peraturan baru serta diperbaikinya peraturan yang tidak lagi relevan. Hingga ditahun 2008 Pemerintah mengeluarkan UU ITE No.11 Tahun 2008 (Abdul Halim Barkatullah dan Teguh Prasteyo, 2005). Namun sayangnya, hukum akan selalu tertinggal satu langkah dari peradaban manusia.

Kejahatan dalam Teknologi selalu mengalami perubahan sehingga Regulasi regulasi hukum yang sudah ada belum dapat melindungi masyarakat sepenuhnya. Majunya dunia Teknologi dan Internet tidak hanya memberikan dampak positif yang berguna untuk mempermudah komunikasi namun juga menyebabkan maraknya kejahatan dalam bidang tersebut. Ada begitu banyak kasus kejahatan yang tercatat melalui teknologi,kejahatan itu dinamakan *Cybercrime*. Adi Hazah membeikan pengertian terhadap cybercrime sebagai tindak kejahatan dengan menggunakan komputer secara illegal (Antoni, 2017). Mulanya *Cybercrime* kerap kali terjadi dalam kegiatan *Ecommerce* , seperti penipuan dan pencurian dalam belanja online, namun ke depanpun *Cybercrime* beralih kepada aspek perbankan.

Jerry Kang mengatakan bahwa batasan terhadap apa yang disebut sebagai data pribadi adalah deskripsi dari informasi yang berkaitan dengan seseorang dan karakteristiknya dapat dibedakan satu sama lain, data tersebut dapat digunakan untuk mengidentifikasi seseorang sehingga keberadaannya sangat utuh (Radian Adi Nugraha, 2012). Pengertian ini masih sejalan dengan pengertian dari data pribadi yang diberikan oleh Pasal 1 Permen Komunikasi dan Infromatika No.20 Tahun 2016 tntang Perlindungan Data Pribadi Dalam Sistem Elektronik, dinyatakan bahwa setiap data perseorangan yang dapat dijamin kebenaran secara nyata dan bersifat melekat terhadap seseorang adalah data pibadi yang harus dijaga kebenarannya serta dijamin kerahasiaannya. Sehingga perlindungan terhadap data-data pribadi merupakan kebutuhan penting dan seharusnya dilakukan secara khusus tentang bagaimana seharusnya Undnag-Undang melindunginya serta bagaimana proses pengumpulan, pendaftaran, penyimpanan, hingga eksploitasi dab penyebarluasan data-data tersebut dilakukan (Sinta Dewi Rosadi, 2015).

Melalui kegiatan perkreditan dan berbagai jasa yang diberikan, bank melayani kebutuhan pembiayaan serta melancarkan mekanisme sistem pembayaran bagi semua sektor perekonomian. Peran yang strategis tersebut terutama disebabkan oleh fungsi utama bank sebagai suatu wadah yang dapat menghimpun dan menyalurkan dana masyarakat secara efektif dan efisien, yang menunjang pelaksanaan pembangunan nasional dalam rangka meningkatkan pemerataan pembangunan dan hasil-hasilnya, pertumbuhan ekonomi dan stabilitas nasional ke arah peningkatan taraf hidup rakyat banyak.”Telah menjadi keyakinan global bahwa peran teknologi informasi berpotensi untuk memberikan kontribusi dalam pembangunan ekonomi, sosial dan budaya. Teknologi informasi juga berpengaruh pada kondisi sosial dimasa akan datang seperti pelayanan medis, pendidikan dan berbagai aspek kehidupan lainnya. Masyarakat saat ini sudah banyak diperkenalkan dengan berbagai kemudahan-kemudahan dalam melakukan kegiatan yang berhubungan dengan proses kehidupan bermasyarakat yang baik dan benar. Jasa yang diberikan oleh pihak perbankan tentunya juga sangat berperan penting didalamnya, selain memberikan kemudahan ternyata hal tersebut juga mempunyai kelemahan-kelemahan yang secara tidak langsung akan merugikan nasabah penggunan jasa dan perbankan yang memberikan pelayanan jasa..’

Pemanfaatan layanan internet banking dalam prakteknya memuat data atau informasi, dimana hal tersebut senantiasa mengalami proses transmisi yang dapat berakibat timbulnya suatu risiko tertentu. Keberadaan hukum dalam hal ini diperlukan guna mengatur berbagai permasalahan dalam penggunaan internet banking, terlebih mengenai *privacy* data atau data pribadi nasabah dalam pemanfaatan layanan internet banking (Tarigan & Paulus, 2019). Pengaturan yang kini diterapkan dalam penyelenggaraan internet banking terbagi atas dua macam model, yaitu *self regulation* dan *government regulation*. *Self regulation* yakni aturan yang lazimnya dibentuk para pihak dalam mengantisipasi kekosongan hukum (*vacum of law*) dalam upaya perlindungan data pribadi, sedangkan government regulation adalah aturan yang lazimnya dibentuk oleh pemerintah dalambentuk undang-undang atau keputusan untuk melindungi data pribadi dan bank. Dalam dunia modern sekarang ini, peranan perbankan dalam memajukan perekonomian suatu negara sangatlah besar. Hampir semua sektor yang berhubungan dengan berbagai kegiatan keuangan selalu membutuhkan jasa bank. Saat ini dan dimasa yang akan datang kita tidak akan bisa lepas dari dunia perbankan, jika hendak melakukan aktivitas keuangan baik perorangan maupun lembaga. Sifat aktifitas internet yang khas dan tidak mengenal batas territorial wilayah negara pada akhirnya, menimbulkan permasalahan mendasar, yaitu menyangkut kemampuan hukum dalam melaksanakan fungsinya melakukan pengaturan dan penegakan sanksi dan bagaimana kemampuan bank dalam melindungi nasabah bank. Namun, kehadiran internet sama sekali tidak bisa dihindari dalam sejarah perkembangan peradaban manusia (Gaib, 2019).

Kehadirannya merupakan bagian dari sejarah perkembangan pemikiran, teknologi, dan ilmu pengetahuan manusia itu sendiri.Perkembangan teknologi informasi, telekomunikasi dan internet menyebutkan mulai munculnya aplikasi bisnis yang berbasis elektronik dalam dunia perbankan sendiri, pada umumnya memanfaatkan teknologi untuk mengakomodir kebutuhan berinteraksi antara perusahaan dengan nasabahnya. Elektronik Banking adalah salah satu jasa bank yang memungkinkan nasabah untuk memperoleh informasi, melakukan komunikasi dan melakukan transaksi perbankan melalui jaringan dan bukan merupakan bank yang hanya menyelanggarakan layanan perbankan melalui internet (Amrillah, 2020). Elektronik banking adalah fasilitas yang disediakan perusaahaan perbankan melalui benda elektronik (Handphone, Komputer dan Telephone) untuk memenuhi kebutuhan bertransaksi perbankan.Reputasi sistem E-Banking didefinisikan sebagai penilaian pelanggan atas keistimewaan suatu sistem secara menyeluruh. Reputasi sistem E-Banking merupakan suatu proses evaluasi menyeluruh pelanggan mengenai kesempurnaan sistem. Perbankan di Indonesia dalan aktivitasnya, wajib mempertimbangkan berbagai permasalah hukum yang mnyertai suatu transaksi perbankan agar tetap mengacu dan tidak bertentangan dengan peraturan perbankan yang ada (Audi & Utomo, 2021).

Kasus pencurian data nasabah perbankan yang terbatu ialah nasabah dari Bank Syariah Indonesia (BSI). Beberapa terakhir ini, sejumlah nasabah Bank Syariah Indonesia atau BSI mengeluh tidak bisa mengakses aplikasi BSI Mobile mereka masing-masing. Menurut perusahaan, pihaknya tengah melakukan *maintenance system* sehingga membuat layanan BSI tidak bisa diakses untuk sementara waktu. Namun belakangan muncul kabar yang mengatakan bahwa BSI jadi korban *ransomware*. Informasi ini pun mencuat lagi di media sosial dipenuhi dengan berbagai bukti bahwa bank tersebut memang terkena ransomware (Prastiwi, 2023).

Hal ini sebagaimana disampaikan oleh pakar keamanan siber sekaligus Pendiri Ethical Hacker Indonesia Teguh Aprianto yang mengungkap kabar BSI diserang ransomware ini melalui akun Twitternya @secgroun, Sabtu (13/5/2023). Lebih lanjut, Teguh mengatakan, total data yang dicuri penjahat siber sebesar 1,5 TB, di antaranya adalah 15 juta data pengguna dan password untuk akses internal dan layanan yang mereka gunakan. Teguh menjabarkan, ormat data yang bocor termasuk di antaranya data karyawan, dokumen keuangan, dokumen ormati, NDA, dan lain-lain. Sementara, data pelanggan yang bocor di antaranya adalah nama, nomor HP, alamat, saldo di rekening, nomor rekening, history transaksi, tanggal pembukaan rekening, informasi pekerjaan, dan lain-lain (Prastiwi, 2023).

Untuk membahas permasalahan yang telah dirumuskan dan dibatasi sebagaimana tersebut diatas, maka dalam metode penyusunan dan penyelesaian peneliti dalam penelitian ini, akan dipergunakan metode dan Teknik penelitian sebagaimana dibawah ini. Jenis penelitian yang dilakukan adalah penelitian yuridis normatif (Suteki dan Galang Taufani, 2018). Sifat penelitian dalam penelitian ini adalah bersifat deskriptif analitis. Jenis data yang digunakan dalam penelitian ini adalah penelitian kepustakaan (*library research*).Sumber data yang digunakan dalam penelitian ini adalah data sekunder yang berupa bahan hukum primer: Undang-Undang Dasar 1945, Kitab Undang-Undang Hukum Perdata, Undang-Undang Nomor 11 tahun 2008 tentang ITE, Undang-Undang Nomor 10 tahun 1998 tentang Perbankan Undang-Undang Nomor 8 tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi, bahan hukum sekunder: yaitu bahan-bahan hukum yang diperoleh buku - buku bacaan dan laporan-laporan hasil penelitian hukum yang ada hubungannya dengan masalah yang diteliti dan bahan hukum tersier yaitu bahan hukum yang pelengkap sifatnya memberikan petunjuk atau penjelasantambahan terhadap bahan hukum primerdan bahan hukum sekunder. Bahanhukum tersier ini terdapat dalam penelitian misalnya kamus hukum, kamus bahasa, ensiklopedia dan lain sebagainya (Soerjono Soekanto & Sri Mamudji, 2001).

### POLA PENYALAHGUNAAN DATA PRIBADI NASABAH DALAM PERSPEKTIF 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 perbankan(Dashora & Patel, 2011) .

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 (Aldriano & Priyambodo, 2022). 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 perbankan antara lain adalah sebagai berikut (Widayanti, 2022):

1. *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.

1. *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.

1. *Sniffing.*

Sniffing cara yang digunakan oleh pelaku dengan mengamati paket data internet yang digunakan oleh pengguna untuk mendapatkan nomor identitas dan password yang bersangkutan

1. *Brute Force Attacking*

yaitu upaya pencurian nomor identitas dan password melalui mencoba kemungkinan atas kombinasi yang dibuat.

1. *Web Deface: System Exploitation,*

yaitu eksploitasi sistem dengan megganti tampilan awal dari sebuah situs resmi.

1. *Email Spamming,*

yakni dengan mengirimkan email kepada pemilik akun dengan menawarkan produk-produk atau menyatakan bahwa pemilik akun telah memenangkan suatu undian.

1. *Denial of Service*, yaitu pelumpuhan sistem elektronik dengan membanjiri akun atau sistem elektronik dengan data dalam jumlah yang besar.
2. *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 (Ratulangi et al., 2021).

1. *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 (Alhakim & Sofia, 2021).

1. *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 yaitu (Arofah & Priatnasari, 2020) :

1. *misuse of card* data yang berupa penyalahgunaan kartu kredit yang tidak dipresentasikan, merupakan kejadian dimana pengguna kartu kredit tidak 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.
4. *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 (Widodo, 2013). *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, 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 (Rompi & Muaja, 2021).

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.

1. *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 (Kurniawan & Hapsari, 2021). Berikut adalah ilustrasi bagaimana alur bagaimana suatu malware dapat menyerang sistem computer 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

1. *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 (Arofah & Priatnasari, 2020).

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 perkembangan zaman

1. **MEKANISME PENGATURAN TINDAK PIDANA TERHADAP PENYALAHGUNAAN DATA PRIBADI NASABAH BANK BSI DALAM RUANG LINGKUP 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 Perbankan.

* + - 1. **Dalam tinjauan 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* (Rompi & Muaja, 2021). 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 Banking milik mereka, jika tidak segera meng upgrade maka internet Banking milik nasabah akan diblokir. Tidak hanya perintah untuk segera mengupgrade *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 (Suci, 2021).

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 (Widayanti, 2022).

* + - 1. **Dalam Tinjauan UU Perbankan**

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 (Widayanti, 2022). 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)” (Satriana, 2019).

* + - 1. **Dalam tinjauan 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 (Habibi & Liviani, 2020). 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 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 (Gulo et al., 2021).

1. **PENUTUP**
2. **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, cardingadalah 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.

1. **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. Perbankan 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.

1. **DAFTAR PUSTAKA**

Abdul Halim Barkatullah dan Teguh Prasteyo. (2005). *Bisnis E-Commerce : Studi Sistem Keamanan dan Hukum di Indonesia* (1st ed.). Pustaka Pelajar.

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber Crime Dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan*, *6*(1).

Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(2).

Amrillah, M. U. (2020). Urgensi Pembentukan Undang-Undang Digital Banking Bagi Perbankan Syariah Di Indonesia. *Jurnal Lex Renaissance*, *5*(4). https://doi.org/10.20885/jlr.vol5.iss4.art12

Antoni. (2017). Kejahatan Dunia Maya (Cybercrime) dalam Simak Online. *Nuraini*, *17*(2), 261–274.

Arofah, N. R., & Priatnasari, Y. (2020). INTERNET BANKING DAN CYBER CRIME : SEBUAH STUDI KASUS DI PERBANKAN NASIONAL. *Jurnal Pendidikan Akuntansi Indonesia*, *18*(2). https://doi.org/10.21831/jpai.v18i2.35872

Audi, M., & Utomo, S. L. (2021). MEDIASI PERBANKAN DALAM PENYELESAIAN SENGKETA ANTARA NASABAH DAN BANK. *SUPREMASI Jurnal Hukum*, *2*(2). https://doi.org/10.36441/supremasi.v2i2.114

Budi Suhariyanto. (2012). *Tindak Pidana Teknologi Informasi*. Rajawali Pers.

Dashora, K., & Patel, P. P. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, *3*(1).

Gaib, D. N. (2019). Dinamika Hukum Perbankan Digital di Indonesia. *Carbohydrate Polymers*, *6*(1).

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2). https://doi.org/10.22437/pampas.v1i2.9574

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2).

Kurniawan, K. D., & Hapsari, D. R. I. (2021). Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia: Analisa Perlindungan Hukum Terhadap Nasabah. *PLENO JURE*, *10*(2). https://doi.org/10.37541/plenojure.v10i2.590

Prastiwi, D. (2023). *4 Fakta BSI Jadi Korban Ransomware, 15 Juta Data Nasabah Dicuri hingga Hacker Minta Tebusan*. Liputan6.Com. https://www.liputan6.com/news/read/5285688/4-fakta-bsi-jadi-korban-ransomware-15-juta-data-nasabah-dicuri-hingga-hacker-minta-tebusan

Radian Adi Nugraha. (2012). *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*. Rajawali Press.

Ratulangi, C. H., Wahongan, D. A. S., & Mewengkang, F. R. (2021). Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan. *Lex Privatum*, *IX*(5).

Rompi, T., & Muaja, H. S. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *IX*(4).

Satriana, I. (2019). KAJIAN YURIDIS TERHADAP KEJAHATAN CYBER DALAM SISTEM PENEGAKAN HUKUM. *Seminar Nasional Inovasi Dalam …*.

Sinta Dewi Rosadi. (2015). *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. PT Refika Aditama.

Soerjono Soekanto & Sri Mamudji. (2001). *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*. Rajawali Pers.

Suci, D. K. (2021). MODUS OPERANDI TINDAK PIDANA PERBANKAN DAN UPAYA PENANGGULANGANNYA DI INDONESIA. *Negara Dan Keadilan*, *10*(2). https://doi.org/10.33474/hukum.v10i2.10862

Suteki dan Galang Taufani. (2018). Metodologi Penelitian Hukum. In *Metodologi Penelitian Hukum*.

Tarigan, H. A. A. B., & Paulus, D. H. (2019). PERLINDUNGAN HUKUM TERHADAP NASABAH ATAS PENYELENGGARAAN LAYANAN PERBANKAN DIGITAL. *Jurnal Pembangunan Hukum Indonesia*, *1*(3). https://doi.org/10.14710/jphi.v1i3.294-307

Widayanti, P. W. (2022). TINDAK PIDANA PENCURIAN DATA NASABAH DALAM BIDANG PERBANKAN SEBAGAI CYBER CRIME. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, *2*(2).

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