YUSTITIABELEN
Volume 10 Nomor 2 Juli 2024
E-ISSN: 2799-5703 P- ISSN :1979-2115

Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital.

Kemal Idris Balaka[1]*, Aulia Rahman Hakim[2], Frygyta Dwi Sulistyany[3]
[1]Teknologi, Politeknik Bina Husada Kendari
[23]Hukum, Fakultas Hukum Universitas Tulungagung
Email Correspondensi: kemalidris1312@gmail.com

Abstrak. *Kemajuan teknologi informasi membawa dampak negatif, mempermudah pelaku kejahatan untuk melancarkan aksinya yang semakin mengkhawatirkan masyarakat di era digital. Dalam penelitian ini terdapat beberapa rumusan masalah, yaitu: (1) Bagaimana modus operandi cybercriminal dalam pencurian data nasabah di sektor perbankan?; (2) Bagaimana pengaturan hukum terkait tindak pidana pencurian informasi nasabah yang dilakukan oleh cybercriminal?; (3) dan Bagaimana upaya pencegahan tindak pidana pencurian data nasabah di sektor perbankan yang dilakukan secara siber?. Untuk menjawab rumusan masalah tersebut, penulis menggunakan penelitian hukum normatif dengan pendekatan yang digunakan mencakup pendekatan perundang-undangan dan pendekatan konseptual, serta mengumpulkan data melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa para pelaku kejahatan memiliki berbagai cara untuk melakukan aksinya, seperti typo site, keylogger, sniffing, brute force attacking, web deface, denial of service, virus, worm, trojan, skimming, carding, phishing, malware dan hacking. Untuk menangani cybercrime, terdapat regulasi yang berlaku, antara lain Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Dalam menangani tindak pidana cyber crime, pemerintah, lembaga non-pemerintah bersama masyarakat mengambil langkah berupa kebijakan penal dan non-penal.*

Kata Kunci : *Kejahatan Siber, Pencurian, Perbankan*

Abstract. *Advances in information technology have had a negative impact, making it easier for criminals to carry out their actions which are increasingly worrying society in the digital era. In this research there are several problem formulations, namely: (1) What is the modus operandi of cybercriminals in stealing customer data in the banking sector?; (2) What are the legal regulations regarding criminal acts of theft of customer information carried out by cybercriminals?; (3) and How are efforts to prevent criminal acts of theft of customer data in the banking sector carried out via cyber? To answer the problem formulation, the author uses normative legal research with the approach used including a statutory approach and a conceptual approach, as well as collecting data through literature study. The research results show that*

criminals have various ways to carry out their actions, such as typo sites, keyloggers, sniffing, brute force attacking, web deface, denial of service, viruses, worms, trojans, skimming, carding, phishing, malware and hacking. To deal with cybercrime, there are regulations in force, including the Criminal Code, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 10 of 1998 concerning Banking . In dealing with cyber crime, the government, non-government institutions together with the community take steps in the form of penal and non-penal policies.

Keywords : *Cyber Crime, Theft, Banking*

Artikel history: Received: 28-07-2024, Revised: 31-07-2024, Accepted: 31-07-2024

PENDAHULUAN

Teknologi saat ini telah menjadi bagian esensial dari kehidupan sosial, dianggap sebagai kebutuhan primer. Salah satu peran utama teknologi adalah sebagai alat pendukung yang memfasilitasi berbagai kegiatan manusia, terutama dalam hal bertransaksi. Teknologi memungkinkan manusia untuk melakukan transaksi dengan lebih efisien dan cepat, mempermudah interaksi ekonomi dan aktivitas lainnya dalam masyarakat modern. Perkembangan teknologi juga diikuti oleh kemajuan internet, yang menjadi pendorong utama munculnya berbagai inovasi di berbagai aspek kehidupan manusia, terutama dalam sektor bisnis. Persepsi masyarakat modern terhadap internet sebagai alat yang sangat penting untuk memenuhi kebutuhan dan pekerjaan mereka lebih efektif dan efisien membuat pengguna internet meningkat setiap tahunnya, hal ini mendorong banyak pihak, termasuk perusahaan dan pengembang teknologi untuk berlomba-lomba menciptakan terobosan baru yang diminati masyarakat (Jusuf & Hermanto, 2019). Salah satu terobosan baru hadir dalam bidang perbankan berupa e-*banking* atau *electronic banking* sebagai layanan perbankan yang menggunakan internet sebagai platform utama untuk menyediakan berbagai layanan kepada nasabah.

Berbagai fasilitas yang disediakan oleh bank melalui layanan internet banking untuk mempermudah kehidupan masyarakat Kemudahan dan kenyamanan dalam melakukan berbagai transaksi keuangan tanpa perlu ke bank telah menjadi nilai tambah yang besar bagi nasabah. Adanya perkembangan internet banking ini mengharuskan sektor perbankan untuk terus meningkatkan kinerja dan fasilitas yang mereka tawarkan yang mana melibatkan peningkatan akan keamanan transaksi online, pelayanan pelanggan yang baik, serta inovasi produk untuk memenuhi kebutuhan nasabah yang semakin kompleks dengan tetap memerhatikan ketentuan dalam Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dalam Undang-Undang Nomor 10 Tahun 1998.

Layanan perbankan yang semakin kompleks ditinjau dari sektor perbankan yang secara universal telah menyediakan layanan e-banking sebagai respons terhadap perubahan gaya hidup masyarakat yang dinamis. Layanan ini sangat cepat dan praktis, sesuai dengan kebutuhan masyarakat yang ingin melakukan transaksi keuangan secara efisien di mana pun dan kapan pun dengan perangkat yang terhubung ke internet, sehingga layanan ini tidak hanya memenuhi kebutuhan akan aksebilitas yang lebih besar, tetapi juga mendukung strategi perbankan dalam bersaing di era digital saat ini (Luthfiatussa'dyah et al., 2022). Industri perbankan sadar bahwa tidak menyediakan layanan elektronik akan membuat mereka tertinggal, sehingga bersaing untuk memberikan fasilitas e-*banking* yang semakin bervariasi, tidak hanya terbatas pada ATM (*Automatic Teller Machine*) tetapi sudah berkembang dalam berbagai macam bentuk pelayanan, seperti phone banking, internet banking, mobile banking dan SMS banking.

Perbankan elektronik muncul sebagai inovasi baru dalam sektor perbankan. Banyak orang mengakses layanan E-*Banking* karena peningkatan signifikan jumlah pengguna internet di Indonesia. Menurut laporan terbaru dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada tahun 2024 jumlah pengguna internet mencapai 221.563.479 orang, dari total populasi

278.696.200 pada tahun 2023. Berdasarkan survei penetrasi internet yang dirilis oleh APJII, tingkat penetrasi internet di Indonesia pada tahun 2024 mencapai 79,5%, meningkat 1,4% dibanding periode sebelumnya. Selain itu, dampak dari pandemi tahun 2020 silam telah memperbesar penggunaan produk perbankan digital karena layanan seperti pembayaran elektronik dianggap dapat mengurangi risiko penularan virus melalui uang kertas maupun logam. Menurut Ahmad Sanusi (2000), dalam artikelnya di Majalah Bank dan Manajemen, menyebutkan bahwa penggunaan Internet Banking dapat mengurangi biaya transaksi hingga 79% dibandingkan dengan biaya transaksi perbankan konvensional (Evi Yani et al., 2018). Selain menghemat biaya, Internet Banking juga menawarkan banyak kemudahan bagi nasabah. Ini termasuk fleksibilitas dalam melakukan berbagai jenis transaksi, baik antara bank dan nasabah, antara bank dengan merchant (penjual), antar bank, maupun antar nasabah.

Perbankan sebagai sektor vital dalam masyarakat menjadikan perbankan rentan terhadap penyalahgunaan wewenang dan tindakan kriminal, baik oleh pihak internal maupun eksternal yang mencoba memanfaatkannya untuk keuntungan pribadi atau kegiatan ilegal. Tindakan kriminal dalam aktivitas perbankan seringkali melibatkan pelanggaran terhadap ketentuan resmi, yang dikenal sebagai tindak pidana perbankan. Karena itu, keamanan sistem perbankan menjadi sangat penting untuk melindungi informasi dan aset keuangan dari ancaman tersebut (Arofah & Priatnasari, 2020).

Dibalik eminensi yang ditawarkan oleh e-banking, disisi lain memicu risiko serius terhadap kejahatan siber yang semakin berkembang sejalan dengan teknologi. Kejahatan siber di sektor perbankan umumnya memiliki tujuan serupa dengan kejahatan konvensional. Tujuan utamanya adalah untuk memperoleh informasi sensitif seperti detail rekening dan kartu kredit nasabah, meretas sistem basis data bank, bahkan hingga melakukan tindakan perampokan bank secara digital. Ini menunjukkan bahwa kejahatan siber

dalam konteks perbankan tidak hanya berfokus pada pencurian data, tetapi juga bisa mencakup aksi-aksi yang mencari keuntungan finansial atau mengganggu operasional lembaga keuangan. Dalam *cyber crime* terdapat dua tipe kejahatan. Tipe pertama melibatkan komputer sebagai target utama dengan mengincar informasi yang disimpan atau diproses oleh komputer untuk tujuan eksploitasi atau penggunaan ilegal lainnya. Sedangkan tipe kedua di mana komputer digunakan sebagai alat untuk melakukan kegiatan kriminal. Contoh-contoh kejahatan ini termasuk pengiriman spam massal, penyebaran malware untuk merusak atau mencuri data, serta serangan DDoS (*Distributed Denial of Service*) yang bertujuan mengganggu layanan online dengan cara membanjiri server target dengan lalu lintas internet yang tidak dapat diatasi.

Ancaman kejahatan siber dalam industri perbankan dapat menyebabkan kerugian signifikan bagi bank dan nasabah. Data pribadi menjadi target utama dalam kejahatan ini, karena informasi pribadi nasabah sangat penting dalam aktivitas perbankan. Pencurian data pribadi di industri perbankan seringkali dilakukan dengan tujuan untuk memperoleh akses ke layanan perbankan korban, yang kemudian dapat dieksploitasi untuk melakukan penipuan atau mencuri saldo nasabah yang berimbas pada kerugian finansial. Menurut survei Mandiant M-Trends 2023, sektor keuangan dan perbankan menjadi target utama serangan kejahatan siber, menempatkannya sebagai salah satu dari tiga sektor terbesar yang sering diserang. Data CPR tahun 2022 menunjukkan tingginya frekuensi serangan siber terhadap sektor ini, dengan sekitar 1.113 serangan setiap minggu secara global. Hal ini menyoroti urgensi perlunya menangani masalah keamanan di sektor perbankan dengan cepat di masa depan. Selain itu, data dari Kementerian Komunikasi dan Informatika (Kominfo) menunjukkan bahwa dari tahun 2017-2022 tercatat 486.000 laporan kejahatan terkait informasi dan transaksi elektronik dengan mayoritas tindak penipuan transaksi online. Berbagai jenis penipuan siber, seperti *malware*, *phishing*, *voice phishing* dan

smishing, juga menjadi ancaman yang kerap mengintai masyarakat dalam konteks keamanan digital.

Data pribadi nasabah adalah informasi yang sangat penting dan harus dilindungi dengan ketat sesuai dengan prinsip kerahasiaan perbankan. Untuk menggunakan layanan transaksi elektronik, nasabah harus memberikan data diri mereka. Hal ini sebagaimana tertuang dalam Pasal 26 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, bahwa penggunaan informasi yang melibatkan data pribadi seseorang seharusnya bergantung pada izin dari orang yang bersangkutan, tetapi saat ini, data pribadi ini belum secara menyeluruh mendapatkan perlindungan yang memadai dari sistem keamanan perbankan.

Di Indonesia, regulasi terkait pencurian data pribadi di sektor perbankan yang dilakukan secara siber secara implisit diatur dalam beberapa undang-undang. Undang-undang yang paling dominan dalam mengatur kejahatan ini adalah Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, terkadang Undang-Undang ini masih memerlukan referensi pada peraturan lain karena sifatnya yang umum, khususnya ketika terjadi masalah di sektor perbankan terkait pencurian data pribadi, akan ada pengacuan pada regulasi lain yang lebih spesifik sesuai dengan bidang tersebut. Kurang ekstensifnya *cyber law* di Indonesia menyebabkan tantangan dalam penyelesaian kasus-kasus kejahatan siber di negara ini. Hal ini karena kurangnya ketentuan yang khusus dan detail mengenai aspek-aspek tertentu dari kejahatan siber, sehingga kadang kala sulit untuk menangani kasus-kasus tersebut dengan efektif.

Berdasarkan latar belakang yang telah diuraikan sebelumnya, muncul rumusan masalah, yaitu: (1) Bagaimana modus operandi *cybercriminal* dalam pencurian data nasabah di sektor perbankan?; (2) Bagaimana pengaturan hukum terkait tindak pidana pencurian informasi nasabah yang dilakukan oleh cybercriminal?; (3) dan Bagaimana upaya pencegahan tindak pidana

pencurian data nasabah di sektor perbankan yang dilakukan secara siber?. Dengan demikian, penelitian akan mempelajari bagaimana kejahatan ini dilakukan, regulasi hukum yang mengaturnya, serta langkah-langkah yang dapat diambil untuk mencegah terjadinya pencurian data nasabah dalam konteks kejahatan siber di sektor perbankan. Adapun tujuan penulis mengangkat kedua permasalahan tersebut adalah untuk mengeksplorasi dan memahami secara mendalam modus operandi *cybercriminal* dalam pencurian data nasabah di sektor perbankan, serta untuk menganalisis kerangka hukum yang mengatur tindak pidana pencurian informasi nasabah yang dilakukan di dunia maya. Selain itu, penelitian juga bertujuan untuk mengidentifikasi dan mengusulkan upaya pencegahan yang efektif guna melindungi data nasabah dari serangan kejahatan siber dalam konteks perbankan modern yang semakin bergantung pada teknologi.

METODE

Metodologi penelitian dalam jurnal ini menggunakan jenis penelitian hukum normatif dengan fokus pada pendekatan perundang-undangan dan pendekatan konseptual. Sumber bahan hukum primer yang digunakan meliputi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 3 Tahun 2011 Tentang Transfer Dana, Undang-Undang Nomor 21 tahun 2011 tentang Otoritas Jasa Keuangan, serta Kitab Undang-Undang Hukum Pidana. Selain itu, bahan hukum sekunder seperti hasil penelitian, tulisan ilmiah, jurnal dan kamus hukum juga digunakan untuk mendukung penelitian ini.

Sedangkan metode pengumpulan data dalam penelitian ini menggunakan studi kepustakaan atau *library research* (Sigit sapto nugroho dkk, 2020). Melalui metode ini pengumpulan data melibatkan pengumpulan dengan cara menganalisis konten yang relevan, termasuk buku, peraturan

perundang-undangan, dokumen dan hasil penelitian yang terkait atau serupa dengan masalah yang diteliti. Pemilihan metode ini bertujuan untuk mengumpulkan informasi dan pemahaman yang mendalam tentang masalah yang sedang diteliti.

HASIL DAN PEMBAHASAN

1. Modus Operandi Pencurian Data Nasabah Di Sektor Perbankan Melalui Kejahatan Siber

Masyarakat selalu bergerak menuju modernisasi, begitu pula hal ini berlaku juga terhadap hukum. Hukum dan masyarakat saling terkait dan harus berkembang bersama agar hukum dapat tetap efektif dalam mengatur kehidupan. Perkembangan teknologi dalam masyarakat akan memengaruhi jenis-jenis kejahatan yang muncul, termasuk meningkatnya kejahatan di ruang virtual atau *cyber crime*. Penggunaan internet yang semakin luas di Indonesia menyebabkan peningkatan kasus kejahatan siber secara signifikan. Cy*ber crime* yang telah merambah ke dunia perbankan, di mana sistem keamanan perbankan masih terus dihadapkan pada tantangan pelanggaran dan penyalahgunaan teknologi tinggi yang harus dihadapi dalam operasional perbankan. Kejahatan siber menggunakan teknologi informasi sebagai alat untuk melakukan tindakan yang melanggar hukum, dan ini menjadi aspek negatif dari perkembangan internet dan teknologi yang pesat.

Dengan kemajuan teknologi, pelaku kejahatan memiliki kemampuan untuk menggunakan platform digital untuk melancarkan aksi kriminal mereka terhadap lembaga perbankan atau individu. Dengan demikian, tantangan keamanan yang dihadapi oleh sektor perbankan tidak hanya berasal dari ancaman fisik, tetapi juga dari risiko yang timbul dari penggunaan teknologi digital untuk tujuan kejahatan. Berbagai jenis *cyber crime* yang umum terjadi dalam sektor jasa perbankan. Kejahatan siber ini dapat mencakup berbagai bentuk serangan digital yang bertujuan untuk mencuri informasi, dana, atau

merusak sistem perbankan. Bentuk-bentuk *cyber crime* yang terjadi tersebut meliputi (Roy, 2022):

a. Typo Site

Situs web palsu yang dibuat dengan nama domain dan alamat yang hampir sama dengan situs resmi. Tujuannya adalah untuk menipu pengguna internet yang membuat kesalahan ketik saat memasukkan alamat situs yang ingin mereka kunjungi. Pelaku kejahatan siber ini memanfaatkan kekeliruan kecil dalam pengetikan untuk mengarahkan pengguna ke situs palsu mereka, yang sering kali dirancang untuk mencuri informasi pribadi, data login, atau detail keuangan.

b. *Keylogger* atau *Keystroke Recorder*

Perangkat lunak atau program yang dirancang untuk mencatat setiap huruf yang diketikkan oleh pengguna pada *keyboard*. Cara kerja *keylogger* adalah dengan merekam semua aktivitas ketikan pengguna secara diam-diam. Informasi yang diketik, seperti nomor identitas dan kata sandi, dapat direkam dan disalahgunakan oleh pelaku kejahatan. Kejahatan ini biasanya terjadi di tempat umum yang menyediakan akses komputer dengan fasilitas internet, seperti warnet, restoran, bandara dan tempat umum lainnya. Di tempat-tempat ini, komputer yang tersedia untuk umum lebih rentan terhadap instalasi *keylogger*.

c. *Sniffing*

Teknik yang digunakan oleh pelaku untuk memantau dan menganalisis paket data yang dikirimkan melalui jaringan internet. Dengan memantau lalu lintas data ini, pelaku dapat menangkap informasi sensitif seperti nomor identitas dan kata sandi pengguna. *Sniffing* bekerja dengan mengintersepsi data yang dikirim antara komputer pengguna dan server. Ini biasanya dilakukan di jaringan yang kurang aman atau tidak terenkripsi, seperti jaringan Wi-Fi publik.

d. Brute Force Attacking

Metode yang digunakan oleh pelaku untuk mencuri nomor identitas dan kata sandi dengan mencoba semua kemungkinan kombinasi secara sistematis. Dalam serangan *brute force*, pelaku menggunakan perangkat lunak otomatis yang mencoba berbagai kombinasi karakter hingga menemukan kombinasi yang tepat. Serangan *brute force* sering kali menargetkan akun dengan kata sandi yang lemah atau umum, karena kombinasi tersebut lebih cepat ditemukan.

e. Web Deface: System Exploitation

Tindakan eksploitasi sistem di mana pelaku meretas dan mengubah tampilan halaman depan dari sebuah situs resmi. Tujuan dari serangan ini adalah untuk merusak reputasi situs, menyampaikan pesan tertentu, atau menunjukkan kerentanan keamanan situs tersebut. Dalam serangan ini, pelaku mendapatkan akses tidak sah ke server atau sistem manajemen konten (CMS) situs web dan mengganti atau memodifikasi konten yang ditampilkan kepada pengunjung.

f. Denial of Service

Serangan yang bertujuan melumpuhkan atau mengganggu kinerja sistem elektronik dengan membanjirinya dengan sejumlah besar data atau permintaan. Dalam serangan DoS, pelaku mengirimkan volume besar data atau permintaan ke server atau jaringan target dalam waktu singkat. Hal ini menyebabkan kelebihan beban pada sistem, sehingga tidak mampu menangani permintaan yang sah dari pengguna lain. Akibatnya, layanan yang disediakan oleh sistem menjadi lambat atau tidak dapat diakses sama sekali.

g. Virus, Worm, Trojan

Jenis *software* yang didistribusikan untuk merusak sistem komputer, mencuri data, memanipulasi informasi, atau melakukan tindakan ilegal lainnya. Tujuan dari penyebaran malware ini adalah untuk merusak sistem komputer, mengakses dan mencuri data sensitif, atau memanipulasi data untuk keuntungan pelaku.

Bentuk-bentuk *cyber crime* yang disebutkan diatas tersebut akan diterapkan dalam modus operandi yang umum digunakan dalam kejahatan pencurian data pribadi di sektor perbankan, meliputi:

a. *Skimming*

Kejahatan di mana pelaku mencuri informasi dari kartu debit atau kredit milik nasabah menggunakan perangkat khusus yang disebut *skimmer*. Proses *skimming* ini dimulai dengan pemasangan *skimmer*, yaitu alat yang dipasang pada mesin ATM untuk merekam data elektronik dari strip magnetic yang terdapat di kartu ATM nasabah saat digunakan. *Skimmer* ini biasanya dipasang dengan cara yang tidak terlihat oleh pengguna ATM. Disamping itu, pelaku juga memasang kamera tersembunyi yang dibuat menyerupai penutup PIN pada mesin ATM untuk merekam nomor PIN yang dimasukkan oleh nasabah. Setelah data elektronik kartu ATM dan nomor PIN berhasil direkam, pelaku kemudian menggunakan informasi tersebut untuk membuat kartu ATM palsu yang identik dengan kartu asli nasabah. Dengan menggunakan kartu palsu dan PIN yang telah direkam, pelaku dapat melakukan penarikan uang atau transaksi lainnya tanpa sepengetahuan nasabah yang bersangkutan (Linggoraharjo, 2020).

b. *Carding*

Tindakan mencuri data kartu kredit dan menggunakan untuk transaksi pembelian secara ilegal di *platfrom* belanja *online*. Carding biasanya dilakukan dengan cara memperoleh informasi kartu kredit korban secara tidak sah, baik melalui pencurian data, penipuan, atau kebocoran data. Modus operandi *carding* ini dimungkinkan karena sistem pengecekan identitas dan keabsahan kartu kredit di toko *online* seringkali tidak cukup kuat atau tidak cukup ketat (Firmansyah, 2021). Oleh karena itu, pelaku dapat dengan mudah menggunakan data kartu kredit yang dicuri untuk berbelanja secara ilegal.

Carding bisa terjadi karena terdapat 4 jenis kasus yang terkait dengan kejahatan siber ini (Zulkarnain & Sutabri, 2023):

1) *Misuse of Card Data*, penggunaan kartu tanpa kehadiran fisik kartu itu sendiri. Penyalahgunaan ini mereka sadari ketika menerima tagihan kartu kredit yang mencatat transaksi yang tidak mereka lakukan;
2) *Wiretapping*, praktik menyadap transaksi kartu kredit untuk memperoleh informasi sensitif, meliputi nomor kartu kredit dan rincian transaksi, yang dikirim melalui jaringan komunikasi;
3) *Counterfeiting*, jenis kejahatan di mana pelaku membuat kartu palsu yang menyerupai kartu kredit asli secara eksternal, baik dalam hal penampilan fisik maupun informasi yang tercetak di atasnya.

c. *Phishing*

Dalam praktik *phishing*, pelaku menggunakan pesan email penipuan yang menyerupai komunikasi resmi dari perusahaan yang sah. Pesan dalam email *phishing* ini seringkali mengarahkan penerima email ke situs web palsu yang dibuat oleh pelaku, atau mencoba membuat penerima email untuk mengungkapkan informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi akun lainnya.

Di ranah perbankan, phising adalah salah satu tindakan melawan hukum dalam *cyber crime* yang menyebabkan *fraund* (penipuan). Penipuan ini umumnya menargetkan kartu kredit dan layanan perbankan online. Dalam kasus penipuan dengan kartu kredit, phishing biasanya bertujuan untuk mendapatkan informasi sensitif seperti nomor belakang kartu kredit dan nomor PIN dari nasabah yang dapat digunakan untuk akses ilegal terhadap rekening untuk melakukan transaksi yang tidak sah (Gulo et al., 2021).

d. *Malware*

Perangkat lunak berbahaya yang tidak dikehendaki dalam sistem komputer. Biasanya, malware dirancang untuk mencuri informasi data atau merusak sistem komputer. Dengan kata lain, malware adalah program atau kode yang dibuat dengan itikad buruk, seperti mencuri informasi sensitif seperti kata sandi atau nomor kartu kredit, merusak file atau sistem operasi, atau mengambil alih kontrol sistem untuk kepentingan yang tidak sah.

Malware dapat mengakibatkan kerusakan serius pada sistem komputer dan dapat menyebabkan kerugian finansial atau kehilangan data bagi pengguna.

Terdapat dua jalur utama di mana sebuah sistem komputer dapat terinfeksi oleh malware, yaitu:

- Melalui *USB Drive*

Sistem komputer dapat terinfeksi malware melalui *USB drive* ketika pengguna menyambungkan perangkat penyimpanan eksternal seperti *flash drive* atau *hard drive* eksternal yang sudah terinfeksi ke dalam komputer. Sistem komputer yang tidak dilengkapi dengan perangkat keamanan seperti antivirus atau program anti-*malware* cenderung lebih rentan terhadap infeksi.

- Melalui Jaringan Internet

Sistem komputer juga dapat terinfeksi *malware* melalui jaringan internet, terutama saat pengguna mengunduh file atau perangkat lunak dari sumber yang tidak terpercaya, mengklik tautan berbahaya dari email *phishing*, atau mengunjungi situs web yang telah dikompromikan. Meskipun sebagian besar email berbahaya biasanya ditangkap oleh *filter spam*, beberapa email tersebut masih bisa masuk ke dalam kotak masuk pengguna. Setelah sistem komputer terinfeksi, *malware* dapat mengakses informasi pribadi, termasuk data perbankan yang tersimpan di dalam komputer.

Kedua jalur tersebut merupakan pintu masuk umum bagi malware ke dalam sistem komputer, maka diperlukan langkah-langkah keamanan yang tepat dengan memastikan untuk memperbarui perangkat lunak antivirus, memperbarui sistem operasi dan perangkat lunak secara berkala, serta tidak membuka email atau mengunjungi situs web yang mencurigakan.

e. *Hacking*

Kejahatan siber di mana pelaku secara ilegal mengakses sistem komputer korban. *Hacker* menggunakan keterampilan teknis mereka untuk melakukan berbagai tindakan kriminal, salah satunya pembobolan kata sandi. *Hacker* dapat menggunakan berbagai teknik, seperti *brute force attack* atau

phishing, untuk mencuri kata sandi pengguna dan mendapatkan akses ke akun atau sistem komputer yang dilindungi oleh kata sandi.

Di ranah perbankan, serangan *Distributed Denial of Service (*DDOS) terjadi ketika para penyerang mengirimkan lalu lintas internet palsu atau permintaan tidak sah ke server perbankan. Tujuan dari serangan ini adalah untuk menghambat atau bahkan menonaktifkan kemampuan server untuk memproses permintaan yang sah dari pengguna yang sebenarnya (Damayanti & Prastyanti, 2024). Akibat serangan tersebut berefek pada gangguan layanan yang signifikan, membuat server tidak responsif terhadap permintaan yang sah dan mengakibatkan kehilangan akses atau penggunaan yang sah atas layanan yang ditargetkan.

Kejahatan di bidang perbankan yang dahulu seringkali dilakukan secara langsung dan nyata seperti, perampokan bank atau pemalsuan dokumen dimana saat ini dapat dilakukan secara virtual dan tanpa batas ruang dan waktu. Perubahan ini menuntut agar sistem pengaturan hukum juga berkembang sesuai dengan perkembangan zaman dan teknologi. Undang-undang yang ada perlu diperbarui dan disesuaikan untuk mengatasi tantangan baru yang dihadapi oleh sektor perbankan akibat kejahatan siber. Perlindungan data pribadi, keamanan transaksi perbankan online, dan penegakan hukum terhadap pelaku kejahatan siber menjadi beberapa aspek yang perlu diperhatikan dalam pengembangan sistem pengaturan hukum yang responsif terhadap perubahan zaman dan teknologi.

2. Pengaturan Terkait Tindak Pidana Pencurian Informasi Nasabah Di Sektor Perbankan Dalam Ranah Kejahatan Siber

A. Tindak Pidana *Cyber Crime* Terkait Pencurian Informasi Nasabah Ditinjau Dari Perspektif Kitab Undang-Undang Hukum Pidana (KUHP)

Dalam konteks penegakan hukum terkait kejahatan siber, terutama pencurian data nasabah di sektor perbankan, ketentuan dalam Kitab Undang-

Undang Hukum Pidana (KUHP) dapat diterapkan dengan melakukan penafsiran yang ekstensif. Beberapa pasal dalam KUHP yang dapat digunakan untuk mengadili kejahatan siber adalah pasal yang mengatur tindak pidana pemalsuan (diatur dalam Pasal 263 sampai dengan Pasal 276), tindak pidana pencurian (diatur dalam Pasal 362 sampai dengan Pasal 367), tindak pidana penipuan (diatur dalam Pasal 378 sampai dengan Pasal 395) dan tindak pidana perusakan barang (diatur dalam Pasal 407 sampai dengan Pasal 412). Sebagai contoh, modus operandi pelaku dalam melakukan pencurian data nasabah melalui teknik phishing. Pelaku mengirimkan email palsu kepada nasabah yang menyatakan bahwa nasabah diwajibkan untuk melakukan upgrade pada layanan internet banking mereka. Email tersebut menciptakan urgensi dengan mengancam bahwa jika nasabah tidak segera melakukan upgrade, layanan internet banking mereka akan diblokir. Selain itu, dalam email tersebut, pelaku mengarahkan nasabah untuk masuk ke sebuah situs web palsu yang dibuat menyerupai situs web asli bank. Nasabah kemudian diminta untuk memasukkan informasi pribadi mereka, seperti *username* dan *password*, untuk melakukan upgrade. Tanpa menyadari bahwa situs web tersebut palsu, nasabah memasukkan informasi pribadi mereka, yang kemudian disadap oleh pelaku. Setelah mendapatkan informasi login nasabah, pelaku menggunakannya untuk mengakses internet banking nasabah dan mentransfer sejumlah uang dari rekening nasabah ke rekening pelaku.

Dalam hal ini, tindakan pelaku dapat diklasifikasikan sebagai penipuan berdasarkan pasal 378 KUHPidana. Pasal ini menyatakan bahwa siapa pun yang dengan sengaja menggunakan nama palsu, tipu muslihat, atau rangkaian kebohongan, untuk mendapatkan keuntungan secara melawan hukum, dengan menggerakkan orang lain untuk menyerahkan barang atau memberikan hutang, dapat dijatuhi pidana penjara maksimal 4 (empat) tahun.

B. Tindak Pidana *Cyber Crime* Terkait Pencurian Informasi Nasabah Ditinjau Dari Perspektif Undang-Undang Nomor 19 Tahun 2016

tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Dalam konteks tindak pidana pencurian data pribadi nasabah, informasi pribadi nasabah menjadi objek yang sangat penting. Di Indonesia, pengaturan mengenai perlindungan terhadap 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). Undang-undang ini memberikan landasan hukum untuk menangani tindak pidana terhadap privasi atau data pribadi, serta memberikan dasar untuk penerapan sanksi hukum terhadap pelaku pencurian data pribadi nasabah, yang diatur dalam beberapa pasal seperti, Pasal 30, Pasal 32 dan Pasal 35 UU ITE. Selain itu, untuk ketentuan pidana, terdapat dalam pasal-pasal lainnya seperti Pasal 46, Pasal 48, Pasal 49 dan Pasal 51 UU ITE. Tindakan yang melanggar hukum, seperti mengakses sistem elektronik untuk memperoleh informasi atau dokumen elektronik dengan melanggar sistem keamanan, dianggap sebagai tindak pidana yang dapat dikenai sanksi pidana penjara antara 6 sampai 8 tahun dan/atau denda maksimum antara Rp 600.000.000,00 sampai Rp 800.000.000,00.

C. **Tindak Pidana *Cyber Crime* Terkait Pencurian Informasi Nasabah Ditinjau Dari Perspektif Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan**

Perlindungan data pribadi nasabah di sektor perbankan dilakukan berdasarkan prinsip kerahasiaan, yang diatur secara tegas dalam Undang-Undang Nomor 10 tahun 1998. Undang-undang ini mengharuskan bank untuk menjaga kerahasiaan informasi pribadi nasabah, termasuk semua detail keuangan dan informasi pribadi lainnya. Pasal 1 ayat (28) dari Undang-Undang Perbankan menegaskan bahwa rahasia bank mencakup segala hal terkait dengan informasi nasabah dan simpanannya.

Selain itu, Pasal 40 ayat (1) Undang-Undang Nomor 10 Tahun 1998 secara khusus mengatur bahwa bank harus menjaga kerahasiaan informasi mengenai nasabah penyimpan dan simpanannya, kecuali dalam keadaan yang diatur secara spesifik dalam pasal-pasal lainnya. Hal ini menunjukkan bahwa perlindungan data pribadi nasabah di sektor perbankan diatur dengan ketat untuk memastikan keamanan informasi nasabah dari akses yang tidak sah atau penyalahgunaan.

Berdasarkan Pasal tersebut, terlihat bahwa bank harus memperlakukan informasi nasabah dengan kerahasiaan yang sangat ketat. Mereka dilarang untuk mengungkapkan atau menyebarkan informasi nasabah ke pihak lain karena dianggap sebagai rahasia bank. Jika terjadi pelanggaran terhadap kerahasiaan informasi nasabah, bank dapat dikenai sanksi sebagaimana tercantum pada Pasal 47 ayat (2) Undang-Undang Perbankan. Pasal 47 ayat (2) tersebut menjelaskan bahwa anggota Dewan Komisaris, Direksi, pegawai bank, atau pihak terafiliasi lainnya yang dengan sengaja memberikan informasi yang seharusnya dirahasiakan menurut Pasal 40, dapat dikenakan 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)".

Dengan meningkatnya kompleksitas dan tingkat kecanggihan kejahatan di bidang teknologi informasi yang sering kali tidak terikat oleh batas-batas geografis, pemerintah perlu proaktif dalam merumuskan dan memperbarui regulasi. Hal ini untuk memastikan bahwa hukum dapat mengatasi perkembangan baru dalam kejahatan siber dan melindungi masyarakat secara efektif.

Meskipun ada regulasi yang mengatur tindak pidana di bidang teknologi informasi, kejahatan di era digital memiliki karakteristik yang berbeda dan seringkali memerlukan pendekatan hukum yang lebih canggih dan adaptif, maka memerlukan regulasi khusus di luar KUHPidana karena perkembangan teknologi yang cepat. Oleh karena itu, diperlukan pengaturan

yang tersendiri untuk menangani isu ini (Koto, 2021). Dari segi hukum, hal ini menuntut pemahaman yang mendalam tentang hukum pidana di Indonesia. Rene David menyatakan bahwa Indonesia menganut "sistem hukum campuran" (Gozali, 2020), yang mencampurkan elemen-elemen dari berbagai sistem hukum, pengaruh dari sistem hukum kontinental, terutama dalam konteks hukum publik dan hukum pidana, yang tampak lebih dominan. Dalam konteks kejahatan siber, ada kebutuhan yang mendesak untuk mengintegrasikan pendekatan hukum yang komprehensif dan terpadu. Hal ini dapat dicapai melalui revisi atau perombakan menyeluruh terhadap Kitab Undang-Undang Hukum Pidana (KUHP), agar lebih sesuai dan relevan dalam menghadapi tantangan dari kejahatan di dunia maya.

3. Pencegahan Tindakan *Cyber Crime* Dalam Pencurian Informasi Nasabah Dalam Ranah Perbankan

Pencegahan dan penanganan *cyber crime* dalam konteks kebijakan kriminal dapat dilakukan dengan dua metode, yaitu (Zaidan, 2016):

1. Kebijakan Penal (*Penal Polic*y)

Kebijakan penal (*penal policy*) menurut Marc Ancel, mencakup aspek ilmu dan seni yang bertujuan membantu legislator dan pengadilan dalam membuat keputusan yang tepat terkait penerapan hukum positif. Ini menekankan pentingnya supremasi hukum dan tanggung jawab pihak-pihak dalam penegakan hukum (Pristiono, 2020). Kebijakan hukum pidana merupakan bagian dari upaya yang tidak hanya terbatas pada penerapan sanksi terhadap pelanggar hukum, tetapi juga meliputi upaya pencegahan dan penanggulangan kejahatan secara menyeluruh. Marc Ancel berpendapat bahwa kebijakan hukum penal haruslah holistik, mencakup srategi pencegahan yang proaktif, agar dapat secara efisien menangani tantangan kejahatan dalam masyarakat modern.

Konsep “Kebijakan Kriminalisasi”, disini sebagai proses di mana tindakan yang sebelumnya legal menjadi ilegal melalui undang-undang. Ini

merupakan bagian dari kebijakan hukum pidana yang lebih luas, yang bertujuan untuk mengatur perilaku masyarakat (Amrani, 2019). Sejak Proklamasi Kemerdekaan Indonesia, proses ini terus berlangsung, dan terdapat banyak delik baru yang diatur dalam Undang-Undang Nomor 1 Tahun 1946. Penciptaan delik baru ini mencerminkan kebutuhan untuk menanggapi perubahan budaya dan iklim politik pada waktu itu, menunjukkan adaptasi hukum terhadap realitas sosial yang berkembang.

Alasan mengapa suatu perilaku tertentu dapat dijadikan delik atau dikriminalisasi, yaitu (Amrani, 2019):

a. Adanya reaksi sosial yang menilai tindakan tersebut tidak sesuai dengan nilai atau norma yang berlaku dalam masyarakat, berupa ketidaksenangan, kekhawatiran, atau penolakan terhadap perilaku tersebut;
b. Perbuatan dapat merugikan masyarakat secara umum yang berdampak pada ekonomi, sosial, atau psikologis yang signifikan terhadap individu atau kelompok dalam masyarakat.
c. Seringnya perilaku itu terjadi dan menimbulkan dampak negatif yang konsisten terhadap masyarakat yang kemungkinan besar perilaku dianggap sebagai delik atau diskriminalisasi.
d. Adanya bukti memadai tentang terjadinya perilaku tersebut juga menjadi pertimbangan penting dalam proses penegakan hukum.

Meskipun terdapat empat kriteria untuk menentukan mengapa suatu perilaku dapat dikriminalisasi, tidak semua tindakan yang tidak diinginkan memenuhi syarat untuk dianggap sebagai kejahatan. Proses kriminalisasi merujuk pada upaya untuk menjadikan suatu tindakan ilegal, dan dengan meningkatnya kecenderungan ini, maka diperlukan pembuatan undang-undang pidana baru. Dampaknya, metode yang digunakan dalam penegakan hukum pidana akan mempengaruhi secara langsung bagaimana proses kriminalisasi berlangsung.Upaya penegakan hukum pidana oleh lembaga kenegaraan yang berwenang. Proses daripada kebijakan penal ini meliputi tiga

tahapan utama yaitu formulasi (penyusunan undang-undang), aplikasi (penerapan hukum oleh penegak hukum seperti polisi dan jaksa) dan eksekusi (pelaksanaan hukuman oleh lembaga pemasyarakatan) yang melahirkan tujuan untuk membentuk satu kesatuan yang menyeluruh tidak hanya dalam menegakkan aturan hukum, tetapi juga mendukung kebijakan sosial (*Social Policy*) yang lebih luas, seperti menciptakan kesejahteraan sosial dan memberikan perlindungan kepada masyarakat secara kolektif.

Beberapa kebijakan penal yang telah dilaksanakan untuk menangani kasus pencurian data pribadi di sektor perbankan sebagaimana berikut.

a. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Undang-undang ini mengatur tentang operasional dan perlindungan nasabah dalam sektor perbankan di Indonesia.
b. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini mengatur penggunaan teknologi informasi dan transaksi elektronik, serta memberikan perlindungan terhadap keamanan dan privasi data pribadi, termasuk data yang disimpan oleh lembaga keuangan seperti bank.
c. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK). Undang-undang ini mengatur tentang pengawasan dan regulasi terhadap industri jasa keuangan di Indonesia, termasuk perbankan. OJK bertanggung jawab untuk memastikan perlindungan nasabah dan stabilitas sistem keuangan.
d. Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah. Undang-undang ini mengatur tentang operasional dan perlindungan nasabah dalam sektor perbankan syariah di Indonesia.
e. Undang-Undang Nomor 24 Tahun 2004 tentang Lembaga Penjamin Simpanan (LPS). Undang-undang ini mengatur tentang lembaga yang bertugas menjamin simpanan nasabah untuk mempertahankan kepercayaan terhadap sistem perbankan di Indonesia.

2. Kebijakan Non-Penal (*Non-Penal Policy*)

Pendekatan atau strategi untuk mengatasi masalah sosial atau mencapai tujuan tertentu tanpa mengandalkan hukuman atau sanksi pidana. Tujuan daripada kebijakan ini ialah mencegah terjadinya kejahatan melalui berbagai cara seperti edukasi, pemberdayaan masyarakat, dan tindakan preventif lainnya yang tidak melibatkan proses peradilan pidana.

Kebijakan ini dilakukan dengan upaya yang tidak melibatkan proses hukum pidana, terdapat beberapa hal yang bisa dilakukan terkait pencegahan melalui kebijakan ini, yaitu:

a. Kerjasama Internasional

Menyoroti pentingnya kerjasama Internasional dalam menghadapi kejahatan cyber yang bersifat lintas negara (transnasional), karena kejahatan *cyber* sendiri yang tidak mengenal batas geografis, maka diperlukan kerjasama yang intensif di tingkat internasional, meliputi beberapa aspek:

- Penegakan Hukum Pidana

  Kolaborasi antar negara dalam penegakan hukum untuk menangkap dan menghukum pelaku kejahatan *cyber*, termasuk mekanisme ekstradisi dan bantuan hukum timbal balik
- Pengembangan Teknologi dan Jaringan Informasi

  Pembentukan sistem jaringan informasi yang kuat dan dapat diandalkan, contohnya melalui program "24 *hours point contact*", di mana program ini dirancang untuk memfasilitasi komunikasi yang cepat dan koordinasi yang efektif antar negara dalam menghadapi ancaman *cyber*.
- Pelatihan Personil Penegak Hukum

  Melatih personel penegak hukum agar memiliki keterampilan dan pengetahuan yang memadai dalam menangani kejahatan *cyber*.
- Harmonisasi Hukum

Menyelaraskan peraturan dan undang-undang antar negara untuk memastikan bahwa kejahatan *cyber* dapat ditangani secara efektif di berbagai yurisdiksi.

- Penyebarluasan Kesepakatan Internasional

  Menyebarkan dan mengimplementasikan kesepakatan internasional terkait kejahatan *cyber* agar ada standar dan prosedur yang konsisten di seluruh dunia.

Kerjasama ini bertujuan untuk memperkuat respons global terhadap kejahatan *cyber*, meningkatkan keamanan digital dan memastikan bahwa pelaku kejahatan tidak dapat memanfaatkan perbedaan hukum dan teknologi antar negara.

3. Rencana Aksi Nasional

Melalui kerjasama antara pemerintah dan komunitas teknologi informasi nasional yang didukung dengan pendirian Indonesia *Forum on Information for Infocom Incident Response and Security Team* (ID FIRST). Sebuah forum atau organisasi yang dibentuk untuk menciptakan sinergi antara berbagai pihak, termasuk pemerintah, kepolisian dan industri teknologi informasi dalam menghadapi tantangan keamanan informasi, terutama dalam upaya pencegahan dan penanganan insiden keamanan siber.

KESIMPULAN DAN SARAN

A. KESIMPULAN

1. Perkembangan teknologi memengaruhi modus operandi kejahatan, khususnya di bidang perbankan. Kejahatan yang sebelumnya dilakukan secara konvensional kini beralih ke metode *cyber crime* (kejahatan dunia maya), yang menimbulkan tantangan besar terutama dalam hal pencurian data pribadi nasabah. Beberapa modus operandi dalam pencurian data pribadi nasabah melalui cyber crime yang sering terjadi di sektor perbankan, yaitu (1) *Skimming*; (2) *Carding*; (3) *Phishing*; (4) *Malware*; dan (5) *Hacking*.

2. Pengaturan mengenai *cyber crime* di Indonesia belum diatur secara rinci dalam undang-undang khusus yang mengatur seluruh aspek *cyber crime*. Saat ini, regulasi yang secara eksplisit berkaitan dengan kejahatan siber di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Namun, untuk kasus pencurian data pribadi di sektor perbankan yang dilakukan melalui kejahatan *cyber*, undang-undang lain seperti undang-undang perbankan dan Kitab Undang-Undang Hukum Pidana (KUHP) juga dijadikan rujukan. Hal ini bahwa dalam menangani kasus pencurian data pribadi di bidang perbankan, berbagai peraturan yang relevan digunakan bersama-sama. Penyelesaian tindak pidana *cyber crime* di Indonesia, termasuk pencurian data pribadi di perbankan, dilakukan dengan mengacu pada pasal-pasal yang terdapat dalam UU ITE. Namun, selama proses pengadilan, ketentuan dalam undang-undang lain yang sesuai dengan tindak pidana tersebut juga dipertimbangkan dan diterapkan.
3. Dalam pencegahan dan penanggulangan tindak pidana cyber crime dalam kasus pencurian data pribadi nasabah dapat ditempuh melalui dua langkah utama yaitu secara kebijakan penal (*Penal Policy*) dan kebijakan non-penal (*Non-Penal Policy*). Secara Penal Policy dimana pencegahan tersebut dilakukan melalui penerapan hukum pidana atau melalui sistem peradilan, hal ini telah diimplementasikan melalui berbagai ketentuan pidana yang terdapat dalam beberapa undang-undang seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan regulasi lain yang mengatur tentang pencurian data pribadi dan kejahatan di bidang perbankan. Sedangkan, dilihat dari *Non-Penal Policy* sebagai pendekatan atau strategi untuk mengatasi masalah sosial tanpa mengandalkan

hukuman atau sanksi pidana, melainkan lebih fokus pada pencegahan, pendidikan, rehabilitasi, atau stimulasi sosial.

B. SARAN

Untuk menghadapi tantangan teknologi yang terus berkembang, diperlukan pembaruan regulasi hukum yang mampu mengakomodasi dinamika kehidupan masyarakat. Oleh karena itu, penulis mengharapkan agar legislator bersama ahli pidana untuk merumuskan regulasi tersendiri yang masif dan komprehensif, mengingat hal ini penting untuk memastikan penegakan hukum yang efektif, terutama terkait pencurian data pribadi di sektor perbankan melalui kejahatan siber. Sebagai lembaga yang memegang peranan penting dimana tugasnya ialah menghimpun dan menyalurkan dana masyarakat, perbankan harus meningkatkan sistem keamanan komputer mereka kuat dan tidak rentan terhadap serangan siber yang terus berkembang.

DAFTAR RUJUKAN

Amrani, H. (2019). *Politik Pembaruan Hukum Pidana*. Yogyakarta: UII Press.

Gozali, D. S. (2020). *Pengantar Perbandingan Sistem Hukum (Civil Law, Common Law, dan Hukum Adat)*. Bandung: Nusa Media.

Nugroho, Sigit Sapto, et. al., (2020). *Metodologi Riset Hukum*. Sukoharjo: Oase Pustaka.

Roy, D. S. (2022). *Cyber Law*. Bandung: CV. Cakra.

Zaidan, M. A. (2016). Kebijakan Kriminalitas. Jakarta Timur: Sinar Grafika.

Arofah, N. R., & Priatnasari, Y. (2020). Internet Banking Dan Cyber Crime : Sebuah Studi Kasus Di Perbankan Nasional *Jurnal Pendidikan Akuntansi Indonesia, Vol. 18, No. 2, Tahun 2020*. *18*(2), 107–119.

Damayanti, A., & Prastyanti, R. A. (2024). Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia. *Multidisciplinary Indonesian Center Journal (MICJO)*, *1*(2), 1043–1054.

https://doi.org/10.62567/micjo.v1i2

Evi Yani, Ade Fitria Lestari, Hilda Amalia, & Ari Puspita. (2018). Pengaruh Internet Banking Terhadap Minat Nasabah Dalam Bertransaksi Dengan Technology Acceptance Model. *Jurnal Informatika*, *5*(1), 34–42.

Firmansyah, N. M. I. & L. N. (2021). Pertanggungjawaban Pidana Carding Terhadap Pengguna Kartu Kredit. *Jurnal Mimbar Keadilan*, *14*(2), 206.

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), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Jusuf, C. S., & Hermanto, D. R. (2019). Apakah Iklan Televisi Masih Kuat Mempersuasi Konsumen Di Era Teknologi, Komunikasi, Dan Informasi. *Jurnal Ilmiah Bisnis Dan Ekonomi Asia*, *13*(1), 37–45. https://doi.org/10.32812/jibeka.v13i1.100

Koto, I. (2021). Cyber Crime According to the ITE Law. *IJRS: International Journal Reglement & Society*, *2*(2), 903–110. http://jurnal.bundamediagrup.co.id/index.php/ijrs

Linggoraharjo, V. (2020). Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming. *Jurnal Magister Hukum ARGUMENTUM*, *7*(1), 34–46. https://doi.org/10.24123/argu.v7i1.3013

Luthfiatussa'dyah, D., Kosim, A. M., & Devi, A. (2022). Strategi Optimalisasi Digitalisasi Produk Perbankan pada Bank Syariah Indonesia. *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam*, *4*(3), 783–802. https://doi.org/10.47467/elmal.v4i3.2073

Pristiono, A. (2020). Kebijakan Kriminal (Criminal Policy) Dengan Konsep Mediasi Dalam Proses Penyidikan Tindak Pidana Umum (Penipuan Dan Penggelapan) Pada Bagwassidik Ditreskrimum Polda Sumut. *Jurnal Ilmiah Muqoddimah: Jurnal Ilmu Sosial, Politik Dan Hummanioramaniora*, *4*(1), 34. https://doi.org/10.31604/jim.v4i1.2020.34-43

Zulkarnain, Z., & Sutabri, T. (2023). Analisis Kejahatan Carding Pada BNI 46.

Blantika : Multidisciplinary Journal, *2*(1), 33–43. https://doi.org/10.57096/blantika.v2i1.10