KEJAHATAN PENCURIAN IDENTITAS KARTU KREDIT MELALUI MODUS *CYBER PHISING* DALAM SEKTOR PERBANKAN

Ni Putu Yesi Ramantari, Fakultas Hukum Universitas Udayana,
e-mail: yesiramantari@gmail.com
I Made Walesa Putra, Fakultas Hukum Universitas Udayana,
e-mail: walesa_putra@unud.ac.id

DOI: KW.2024.v14.i01.p5

ABSTRAK

Tujuan dalam penulisan ini adalah untuk mengkaji hal sebagai berikut: (1). menganalisis dan menyelidiki terkait pencurian identitas kartu kredit dengan menggunakan metode cyber phising berdampak pada pelanggan perbankan; dan (2). menganalisis untuk menggali informasi tentang perlindungan hukum yang ada dalam melindungi pelanggan perbankan dari ancaman pencurian identitas kartu kredit melalui modus cyber phising. Metode dalam studi ini menggunakan metode pendekatan normatif dari perspektif internal yuridis menggunakan literatur-literatur dan peraturan perundang-undangan yang berkaitan dengan masalah yang diteliti. Hasil studi menunjukan bahwa adanya ancaman terhadap pencurian identitas kartu kredit dengan metode cyber phising di bidang perbankan dan berdampak negatif terhadap pelanggan perbankan yang mengalami kerugian secara finansial. Perlindungan hukum yang dihadirkan oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) meskipun tidak secara khusus mengatur mengenai kejahatan cyber phising, terutama masalah kejahatan pencurian identitas kartu kredit, namun undang-undang tersebut dapat dijadikan rujukan yang memberikan kerangka hukum untuk melindungi pengguna kartu kredit dari berbagai bentuk kejahatan elektronik, terutama kejahatan yang berhubungan dengan aktivitas cyber phising.

Kata Kunci: *Kejahatan, Pencurian, Kartu Kredit, Cyber Crime, Cyber Phising*

ABSTRACT

The aim of this writing is to examine the following: (1). analyzing and investigating credit card identity theft using cyber phising methods that impact banking customers; and (2). analyze to dig up information about existing legal protections to protect banking customers from the threat of credit card identity theft through cyber phising. The method in this study uses a normative approach from an internal juridical perspective using literature and statutory regulations related to the problem under study. The study results show that there is a threat of credit card identity theft using cyber phising methods in the banking sector and has a negative impact on banking customers who experience financial losses. The legal protection provided by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) although it does not specifically regulate cyber phising crimes, especially the crime of credit card identity theft, however This law can be used as a reference that provides a legal framework to protect credit card users from various forms of electronic crime, especially crimes related to cyber phising activities.

Keywords: *Crime, Theft, Credit Card, Cyber Crime, Cyber Phising*

I. Pendahuluan

1.1. Latar Belakang Masalah

Perkembangan masyarakat di era sekarang ini merupakan bagian yang tak terpisahkan dari proses modernisasi yang terikat dengan teknologi informasi yang inovatif. Pesatnya perkembangan teknologi dan informasi semakin mengubah kebutuhan dan gaya hidup masyarakat yang bergantung pada teknologi. Internet menjadi salah satu aspek dengan kemajuan yang sangat cepat dan menjadi bagian penting atau keharusan dalam kehidupan masa kini. Kondisi ini juga yang mempengaruhi perkembangan kejahatan. Sudah banyak insiden terkait kasus kejahatan dunia maya (*cyber crime*) di Indonesia, mulai dari penipuan, pencurian identitas, dan ancaman tagihan utang palsu yang tidak pernah dilakukan.[1]

Peningkatan sistem informasi teknologi, terutama dalam komputer dan internet memang telah terbukti membawa dampak positif bagi perkembangan kehidupan manusia dari berbagai bidang. Ketersediaan informasi yang mudah dan cepat menjadi salah satu keunggulan dari perkembangan tersebut.[2] Akan tetapi, walaupun perkembangan teknologi dan informasi internet memiliki dampak positif, sebaliknya terdapat sisi negatif juga yang umum timbul seperti penggunaan yang salah dari teknologi tersebut yang menjadi sarana efektif untuk melakukan tindak kejahatan dunia maya (*cyber crime*). Seperti contohnya penggunaan penyimpangan oleh individu ataupun kalangan tertentu yang memiliki keinginan untuk menembus jaringan atau situs milik orang lain dengan maksud menyalahgunakan data, mencuri data pribadi, mengubah atau mendapatkan akses ke data pribadi milik orang lain untuk tujuan penjualan data pribadi, penipuan, dan kegiatan-kegiatan lainnya.

Penggunaan yang menyimpang dalam dunia teknologi juga sering terjadi salah satunya dalam sektor perbankan. Berbagai kejahatan tindakan kriminal (ilegal) dalam perbankan biasanya meliputi pencurian identitas pribadi seseorang, seperti nomor kartu kredit atau data identitas yang kemudian digunakan untuk melakukan penipuan keuangan. Misalnya kejahatan dalam kategori kartu kredit cangkupannya relatif luas dengan karakteristik khusus terkait penggunaan media digital komputer yang terhubung dengan suatu jaringan internet global di seluruh penjuru dunia.[3] Awal mulanya sejak tahun 2003, telah ada banyak kasus-kasus kejahatan yang muncul menggunakan pemanfaatan teknologi informasi, diantaranya kejahatan *carding* (penipuan kartu kredit), *phising*, *skimming* ATM/EDC, perjudian online, dan berbagai kejahatan lainnya. *Cyber crime* memiliki potensi untuk dijalankan dengan gampang dan lebih manjur berkat adanya kemajuan teknologi dan informasi yang mengakibatkan penipisan batas privasi yang membuat data pribadi menjadi lebih mudah tersebar secara luas.[4]

Pencurian data/identitas kartu kredit adalah sebagian bentuk kejahatan *cyber* yang umumnya terjadi dalam industri perbankan, seperti *carding* atau *card skimming*.

---

[1] DM, Mohd. Yusuf., Vivi Yola, Destin Maiharani, and Egi Dwi. "Analisis Terhadap Modus-Modus Dalam Hukum *Cyber Crime*." *Jurnal Hukum, Politik dan Ilmu Sosial (JHPIS)* 1, No. 2 (2022): 64-70.

[2] Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *Jurnal SASI* 27, No. 1 (2021): 38-52.

[3] Rustam. "Tinjauan Yuridis Terhadap Tindak Pidana Pencurian Kartu Kredit Dengan Menggunakan Internet di Indonesia." *Jurnal Trias Politika* 4, No. 2 (2020): 229-237.

[4] Rumlus, Muhamad Hasan, and Hanif Hartadi. "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik." *Jurnal HAM* 11, No. 2 (2020): 285-299.

Selain dua jenis kejahatan tersebut, ada juga salah satu bentuk kejahatan lain yang dikenal sebagai *phising*. "*Phising* adalah upaya untuk menyamar sebagai sebuah situs dengan tujuan untuk melakukan penipuan".[5] Dengan kata lain, *phising* adalah kegiatan memperdaya seseorang dengan cara memancing atau menarik orang melalui penipuan, sehingga secara tidak sadar orang tersebut menyerahkan segala informasi yang diperlukan oleh pelaku kejahatan.

Phising termasuk dalam kategori kejahatan *cyber* yang saat ini banyak dilakukan melalui jaringan komputer. Tindakan penjahat *cyber* yang umumnya dilakukan adalah serangan dengan menyisipkan tautan palsu pada akun media sosial, seperti melalui email, pesan SMS, atau bahkan melalui telepon yang mengundang dengan ajakan atau iklan menarik. Dengan hal tersebut, penjahat dapat mengambil dan mengakses informasi pengguna dan memanfaatkannya untuk keuntungan pribadi, seperti mengambil uang, nomor rekening dan nomor kartu kredit pengguna yang kemudian digunakan untuk pembayaran online. Langkah yang paling sederhana yang dapat dilakukan untuk mengantisipasi serangan *phising* adalah dengan tidak membuka tautan yang diterima melalui akun media sosial ataupun akun email media sosial. Ada baiknya jika link tersebut dicurigai sebagai serangan *phising* agar dapat terhindar dari konten dan tautan yang menjebak.[6] Dalam konteks kaitannya dengan pencurian kartu kredit, kejahatan *phising* biasanya seringkali digunakan sebagai salah satu bentuk penipuan online yang digunakan untuk merampas data sensitif, seperti nomor kartu kredit di sektor perbankan. Dalam hal ini, pelaku pencurian identitas kartu kredit dengan *cyber phising* akan berupaya untuk membuat korban percaya bahwa mereka sedang berinteraksi dengan lembaga keuangan yang sah, seperti bank, yang nantinya dari hal ini penjahat dapat mengumpulkan informasi pribadi mereka.

Dalam situasi saat ini, tingkat ketergantungan masyarakat pada teknologi informasi semakin meningkat, yang juga berarti risiko yang dihadapi semakin tinggi. Salah satu risiko tersebut adalah penyalahgunaan data pribadi, termasuk pencurian identitas rekening dan kartu kredit yang dapat menyebabkan kerugian bagi mereka yang datanya diambil. Tindakan pencurian, penyalahgunaan, penjualan data pribadi tentu melanggar hukum teknologi informasi dan dapat digolongkan sebagai bentuk pelanggaran terhadap hak asasi manusia, yang dimana seharusnya perlu dijaga dan dilindungi. Dengan adanya peristiwa tersebut, dapat dilihat bahwa dalam kegiatan baik perbankan maupun belanja online yang memerlukan data pribadi memang sangat rentan terhadap penyalahgunaan atau pencurian oleh peretas pihak ketiga. Penyalahgunaan data pribadi merupakan perbuatan yang mencangkup aspek kejahatan, seperti pencurian dan penipuan.

Berdasarkan permasalahan diatas, diperlukan adanya peraturan-peraturan atau kebijakan-kebijakan yang mengatur mengenai kejahatan dunia maya, terutama dalam bentuk serangan kejahatan *phising*. Di Indonesia sendiri sebetulnya telah memiliki Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang bisa dijadikan rujukan terhadap kejahatan semacam ini.[7] Dengan demikian, penulis

---

[5] Tim Indonesia baik.id. *Tips Praktis di Dunia Siber* (Jakarta, Direktorat Jenderal Informasi dan Komunikasi Publik Kementerian Komunikasi dan Informatika, 2019), 21.

[6] Wibowo, Mia Haryati, and Nur Fatimah. "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime." *Jurnal of Education and Information Communication Technology* 1, No. 1 (2017): 1-5.

[7] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

berkeinginan untuk mengkaji lebih dalam persoalan tersebut dengan sebuah penelitian yang berjudul "Analisis Yuridis Kejahatan Pencurian Identitas Kartu Kredit Melalui Modus *Cyber Phising* Dalam Sektor Perbankan". Pembahasan mengenai penyalahgunaan dan pencurian data identitas kartu kredit disini memang bukanlah merupakan hal yang baru, karena sebelumnya terdapat beberapa penelitian terdahulu yang ada kaitannya dengan permasalahan yang diangkat dan dibahas dalam mendukung penelitian ini, diantaranya yaitu: "Analisa Kasus *Cybercrime* Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit" karya milik Nunuk Sulisrudatin. Dalam kajian tersebut berfokus pada tindak kejahatan *cyber crime* di sektor perbankan yang berhubungan dengan pencurian data kartu kredit dan menekankan pada upaya-upaya untuk pencegahan tindak pidana tersebut. Sementara itu, kajian milik Galang Ramadhan Djokdja, Sherly Adam, dan Margie Gladies Sopacua mengkaji "Pertanggungjawaban Pidana Pelaku Pembobolan Kartu Kredit Dalam Tindak Pidana di Bidang Perbankan" yang dimana fokusnya menekankan pada pengaturan hukum pidana dan pertanggungjawaban pidana bagi pelaku pembobolan kartu kredit dalam tindak pidana perbankan. Berbeda dengan penelitian sebelumnya, fokus penelitian dari penulis kali ini lebih berfokus kepada mekanisme dan strategi yang digunakan dalam kejahatan *cyber phising* untuk mencuri identitas kartu kredit korbannya. Selain itu, penelitian ini juga mengevaluasi pengaruh atau dampak pencurian identitas kartu kredit dengan modus *cyber phising* bagi pelanggan perbankan, serta menganalisis perlindungan hukum yang ada dalam melindungi pelanggan perbankan dari ancaman pencurian identitas kartu kredit melalui modus *cyber phising*.

1.2. Rumusan Masalah

Berdasarkan latar belakang permasalahan yang diuraikan, diperoleh rumusan masalah, yaitu sebagai berikut:

1. Bagaimanakah pencurian identitas kartu kredit dengan menggunakan modus/metode *cyber phising* dalam bidang perbankan, serta pengaruh atau dampaknya terhadap pelanggan perbankan?
2. Bagaimanakah perlindungan hukum dalam melindungi pelanggan dari ancaman pencurian identitas kartu kredit melalui modus *cyber phising*?

1.3. Tujuan Penulisan

Tujuan dalam penulisan artikel ini adalah untuk menganalisis dan menyelidiki terkait pencurian identitas kartu kredit dengan menggunakan metode *cyber phising* berdampak pada pelanggan perbankan, serta menganalisis dan menggali informasi tentang perlindungan hukum dalam melindungi pelanggan perbankan dari ancaman pencurian identitas kartu kredit melalui modus *cyber phising*.

II. Metode Penelitian

Jenis metode penelitian ini menggunakan metode pendekatan normatif, yaitu mengkaji dan menganalisis objek hukum dari perspektif internal yuridis dengan menggunakan norma hukum serta literatur-literatur dan peraturan perundang-undangan yang berkaitan dengan masalah yang diteliti. Sumber bahan hukum yang digunakan adalah primer dan sekunder. Sumber hukum primer mengacu pada UUD NRI 1945 dan UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Sedangkan bahan hukum sekunder sebagai pendukung data primer sebagai salah satu sumber data antara lain:

literatur, jurnal hukum atau artikel, serta bahan lainnya yang berkaitan dengan permasalahan yang sedang diteliti.

III. Hasil dan Pembahasan

3.1. Pencurian Identitas Kartu Kredit dengan Metode *Cyber Phising* dalam Bidang Perbankan, serta Pengaruh atau Dampaknya Terhadap Pelanggan Perbankan

Istilah *phising* (*password harvesting fishing*) ini berasal dari Bahasa Inggris "*fishing*" yang memiliki arti memancing.[8] Sebuah aktivitas yang bertujuan untuk memancing guna memperoleh informasi dari pihak lain. Informasi yang diperoleh melalui aktivitas ini meliputi nama pengguna, kata sandi, alamat email, data pribadi, dan lain sebagainya. *Phising* diperkenalkan pada tahun 1995 sebagai bentuk serangan *cyber*. Menurut James (2005), salah satu metode awal yang digunakan oleh para pelaku *phising* adalah dengan algoritma untuk menciptakan nomor kartu kredit secara sembarang. Bentuk *cyber phising* di Internet banking menjadi ancaman serius yang bertujuan untuk menipu pengguna atau pelanggan.[9] Secara khusus, *phising* seringkali ditargetkan pada pengguna layanan perbankan online, karena data pengguna dan kata sandi dapat disalahgunakan oleh pihak lain. Faktor yang menjadi penyebab potensi serangan *phising* dalam layanan keuangan online adalah kurangnya kesadaran masyarakat tentang pentingnya menjaga keamanan data mereka.

Phising melibatkan penipuan dimana pelaku (*scammer*) menjangkau korban dengan menyamar sebagai entitas bisnis yang sah, seperti bank, perusahaan telekomunikasi, atau penyedia layanan internet. Mereka menggunakan berbagai saluran komunikasi seperti email, media sosial, panggilan telepon, atau pesan SMS. Salah satu taktik yang umum digunakan dalam *phising* adalah membuat halaman web palsu yang sangat menyerupai aslinya, dalam praktik yang dikenal sebagai *web cloning*. Apabila seseorang tanpa curiga memasukkan informasi login mereka melalui laman web palsu, data username dan password akan tercatat otomatis oleh penjahat yang melakukan *phising*. Secara umum, teknik ini disebut sebagai fake login, dimana tanpa sadar seseorang masuk ke dalam situs web palsu yang seolah-olah merupakan situs web resmi. Apabila korban secara online atau melalui telepon memberikan rincian data pribadi kepada penipu, mereka akan mengeksploitasi informasi tersebut untuk melakukan aktivitas penipuan, seperti penyalahgunaan kartu kredit dan pencurian dana yang dimiliki oleh korban.[10]

Phisher menelusuri untuk mencari dan mendapatkan informasi seperti password akun atau nomor kartu kredit korban. Metode yang digunakan seperti pengiriman email, menampilkan banner, atau jendela pop-up untuk mengalihkan pengguna ke situs web palsu dengan niat mengungkapkan informasi pribadi pengguna. Adapun untuk mendapatkan korban pencurian identitas kartu kredit melalui *phising*, terdapat berbagai metode yang digunakan. Ada beberapa modus kejahatan yang dilakukan dengan berbagai jenis dan cara kerja seperti berikut:

a. ***Spear Phising* (email *phising*)**: dilakukan dengan melibatkan email yang ditargetkan secara spesifik kepada individu atau kelompok tertentu,

---

[8] Zam, Efvy. *Phising: Cara Mudah Menyadap Password dan Pencegahannya* (Jakarta, Mediakita, 2014), 2.

[9] Muftiadi, Amin, Tri Putri Mulyani Agustina, and Margaretha Evi. "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman *Phising* Terhadap Layanan *Online Banking*." *Jurnal Ilmiah Teknik* 1, No. 2 (2022): 60-65.

[10] H, Monica Shelsa. *Skripsi*: *Analisis Tindak Pidana Pencurian Data Pribadi Melalui Teknik Phising Ditinjau Dalam Perspektif Fiqih Jinayah* (Semarang, Fakultas Syariah dan Hukum Universitas Islam Negeri Walisongo, 2022), 52-53.

dimana pelaku menyamar sebagai organisasi atau perusahaan terpercaya. Pesan email mengandung tautan yang mengarahkan target membuka situs palsu dengan menginformasikan adanya aktivitas yang mencurigakan pada akun kartu kredit target dan meminta target untuk memverifikasi informasi pribadi mereka atau memperbarui rincian akun mereka melalui tautan yang diberikan. Begitu target memberikan informasi, pelaku *phising* akan mendapatkan akses ke kartu kredit mereka untuk melakukan transaksi online yang tidak sah atau melakukan pencurian identitas dengan cara lainnya.[11]

b. **Telepon dan SMS Pesan Singkat**: phising melalui telepon dan sms dilakukan oleh pelaku yang mengaku sebagai pihak yang terkait seperti bank atau penyedia layanan kartu kredit. Mereka akan mengirim tautan palsu dan menanyakan informasi pribadi kartu kredit seperti user ID, password, dan kode OTP.[12]

c. **Website**: pelaku mencuri informasi kartu kredit yang disimpan atau dimasukkan oleh pengguna pada situs web yang tidak sah atau rentan. Situs web palsu meniru tampilan situs web yang sah, seperti situs web perbankan atau situs web *e-commerce* populer. Pelaku dapat menyebarkan malware ke perangkat pengguna melalui unduhan yang berbahaya atau tautan yang meragukan. Malware ini dapat memantau aktivitas pengguna, termasuk saat mereka memasukkan informasi kartu kredit pada situs web, dan mengirimkan data tersebut kepada pelaku.[13]

d. ***Deceptive Phising***: upaya penipuan yang dilakukan dengan menggunakan identitas institusi perusahaan yang dikenal. Pelaku mengirimkan tautan menyesatkan yang tersembunyi dan mirip dengan instansi perusahaan terkenal. Teknik ini bisa digunakan melalui beragam jenis saluran komunikasi, termasuk email, pesan teks, dan WhatsApp. Korban akan diminta untuk memasukkan informasi pribadi dan keuangan mencakup nomor kartu kredit, tanggal kadaluwarsa, kode CVV, serta informasi pribadi lainnya seperti alamat, tanggal lahir, atau nomor identitas.

e. **Trojan**: peretas melibatkan perangkat lunak jahat untuk mencoba masuk ke akun pengguna. Informasi yang dihasilkan kemudian dikirim ke *phisher*. Jenis malware ini menyamar sebagai program atau file yang sah, sehingga mampu menyusup ke dalam perangkat lunak komputer dan menjalankan tindakan yang merugikan. Trojan dapat merekam struk pengguna, mengakses file, atau mengintip aktivitas online korban.[14]

Perlindungan informasi telah menjadi fokus utama di organisasi modern karena kerahasiaan data tersebut menjadi landasan kunci dalam konsep keamanan informasi. Data dianggap sebagai aset berharga yang perlu diselamatkan dari ancaman. Dampak bagi pemilik data pribadi mereka yang tersebar ke tangan yang tidak berwenang

---

[11] Fikri, Adi Wibowo Noor, Achmad Fauzi, Aldi Alfathur Rachman, dkk. "Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phising dalam Layanan Online Banking." *Jurnal Ilmu Multidisiplin* 2, No. 1 (2023): 84-91.

[12] Banjarnahor, Andrew Christian, and Puti Priyana. "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo." *Jurnal Hermeneutika* 6, No. 1 (2022): 32-36.

[13] Wibowo, Mia Haryati, and Nur Fatimah. "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime." *Jurnal of Education and Information Communication Technology* 1, No. 1 (2017): 1-5.

[14] H, Monica Shelsa. *Op. Cit,* 58.

sangatlah serius. Seorang ahli keamanan siber yang menjabat sebagai Ketua *CISSReC* (*Communication & Information System Security Research Center*), menjelaskan bahwa data yang bocor akan mudah bagi penjahat dapat memanfaatkannya melalui serangan *phising* yang disasarkan atau dengan menggunakan metode manipulasi sosial. Dalam praktik *phising*, baik melalui pesan atau situs web, pelaku seringkali mampu meyakinkan korban terkait data yang akurat. Oleh karena itu, peluang pencurian akun korban menjadi sangat mungkin terjadi.[15] Bagi pelanggan perbankan, akan menyebabkan korban kehilangan data dan dana kartu kredit yang dicuri untuk melakukan transaksi yang tidak sah atau menguras saldo di rekening korban. Mereka juga rugi secara finansial yang mungkin harus menanggung biaya dari transaksi yang tidak sah atau kehilangan uang yang dicuri oleh pelaku *phising*. Pelanggan perbankan yang menjadi korban *phising* dapat mengalami kerugian reputasi. Kejadian tersebut dapat mengurangi kepercayaan mereka terhadap institusi perbankan dan menyebabkan dampak negatif pada hubungan dengan lembaga keuangan tersebut.

3.2. Perlindungan Hukum dalam Melindungi Pelanggan dari Ancaman Pencurian Identitas Kartu Kredit Melalui Modus *Cyber Phising*

Pencurian identitas kartu kredit merupakan salah satu pelanggaran terhadap data pribadi. Perlindungan terkait hal tersebut di Indonesia dapat dicermati dalam peraturan-peraturan berikut:

- Pasal 28G ayat (1) UUD NRI 1945:[16] secara tidak langsung juga mengatur perlindungan data informasi pribadi karena hal itu merupakan salah satu bentuk HAM yang harus dilindungi. Perlindungan data pribadi termasuk identitas kartu kredit penting untuk memastikan bahwa individu memiliki kendali atas informasi pribadi mereka dan bahwa informasi tersebut tidak disalahgunakan atau diakses tanpa izin. Setiap orang berhak untuk melindungi privasi serta menjaga kerahasiaan data mereka.
- Pasal 26 UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik: bagian penjelasannya disebutkan, salah satu hak yang dimiliki individu adalah perlindungan terhadap informasi pribadinya.[17] Sementara PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ditegaskan bahwa data individu tertentu akan disimpan, dikelola, dan dijaga agar tetap akurat dan kerahasiaannya terlindungi.[18] Pasal tersebut menjelaskan pentingnya melindungi data pribadi seseorang. Apabila informasi pribadi, termasuk kartu kredit, disalahgunakan tanpa persetujuan pemiliknya, pemilik berhak untuk menuntut ganti rugi atas kerugian yang terjadi. Isi pasal tersebut mengindikasikan bahwa tindakan seperti mengumpulkan dan menyebarkan data pribadi tanpa izin ini melanggar privasi seseorang, karena hak tersebut mencakup keputusan atas pemberian atau tidaknya informasi pribadi, termasuk didalamnya pencurian data/identitas kartu kredit.
- Pasal 28 ayat (1) UU ITE: berhubungan dengan berita bohong, pernyataan dalam pasal tersebut pada dasarnya tidak secara langsung terkait dengan kejahatan pencurian identitas dengan modus *phising*. Isi pasal tersebut menunjukkan perhatiannya terhadap tindakan penyebaran berita bohong dan mengelabui

---

[15] Pusat Ensiklopedia. URL: https://p2k.stekom.ac.id/ensiklopedia/Pratama_Dahlian_Persadha#cite_note-14, diakses pada 7 Juli 2023.

[16] Pasal 28G ayat (1) UUD NRI 1945

[17] Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *Jurnal SASI* 27, No. 1 (2021): 38-52.

[18] PP No. 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

hingga menimbulkan kerugian konsumen dalam transaksi elektronik. Sementara itu, kejahatan pencurian identitas kartu kredit dengan modus *phising* melibatkan praktik menipu untuk memperoleh informasi pribadi korban, seperti halnya nomor kartu kredit melalui pembuatan situs atau pengiriman email palsu. Meskipun keduanya merupakan tindakan kejahatan dalam konteks transaksi elektronik, pernyataan tersebut tidak secara khusus mengacu pada modus *phising* atau pencurian identitas.

- Pasal 35 jo Pasal 51 ayat (1) UU ITE: pasal tersebut tidak secara khusus mengatur tentang *phising*, namun jika dikaitkan dengan Pasal 35 dengan kejahatan pencurian identitas kartu kredit dengan modus *phising*. Dalam modus *phising*, seorang pelaku sengaja dan tanpa wewenang atau melanggar hukum memanipulasi, seperti pembuatan situs web palsu atau pengiriman email palsu untuk mencuri informasi pribadi dan keuangan korban, termasuk data kartu kredit. Pelaku berusaha agar informasi elektronik yang mereka peroleh terlihat otentik dan sah, sehingga mereka dapat menggunakan data tersebut untuk melakukan penipuan atau transaksi yang merugikan korban.[19] Tindakan ini melanggar hak privasi dan keamanan korban serta dianggap sebagai kejahatan. Jika pelaku terbukti melanggar, maka dapat dihukum maksimal 12 tahun penjara dan denda maksimum sebesar 12 miliar (sesuai Pasal 51 UU ITE).

IV. Kesimpulan sebagai Penutup

4. Kesimpulan

Pencurian identitas kartu kredit melalui *phising* menargetkan pengguna layanan perbankan online dimana data pengguna dan kata sandi dapat disalahgunakan oleh pihak lain. Metode *cyber phising* yang digunakan antara lain yaitu *spear phising* (email *phising*), telepon dan SMS pesan singkat, website palsu, *deceptive phising*, dan trojan. Pelaku *phising* menyamar sebagai entitas bisnis yang sah, seperti bank atau perusahaan terpercaya, lalu meminta korban untuk mengungkap data informasi pribadi kartu kredit mereka lewat tautan palsu atau halaman web palsu sebagai penipuan, pencurian identitas, atau penyalahgunaan kartu kredit. Dampaknya akan merugikan pelanggan perbankan. Mereka dapat kehilangan data dan dana yang dicuri untuk transaksi yang tidak sah atau mengalami kerugian finansial lainnya. Mereka juga dapat mengalami kerugian reputasi dan kehilangan kepercayaan terhadap institusi perbankan. Perlindungan hukum terhadap pelanggan dari ancaman pencurian identitas kartu kredit melalui modus *phising* mencakup peraturan dan undang-undang yang pada dasarnya melindungi data pribadi dan privasi individu. Diantaranya menjadi fokus dari UUD NRI 1945 dan UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai dasar hukum yang relevan. Beberapa pasal yang dijadikan rujukan yaitu Pasal 28 G ayat (1) UUD NRI 1945, Pasal 26, 28, 35, dan 51 UU ITE. Peraturan-peraturan tersebut menunjukan pentingnya melindungi dan menjaga kerahasiaan data pribadi. termasuk kartu kredit. Dalam hal ini, pasal-pasal tersebut memang tidak secara langsung memiliki hubungan dengan kejahatan *phising* kartu kredit, sehingga perlu adanya penafsiran lebih lanjut mengenai ketentuan khusus kejahatan *cyber phising*, terutama dalam hal pencurian identitas kartu kredit. Namun, pasal-pasal sebagaimana dijelaskan sebelumnya dapat dijadikan suatu rujukan untuk memberikan kerangka

[19] Gulo, Ardi Saputra, Sahuri Lasmadi, and Kabib Nawawi. "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik." *PAMPAS: Journal Of Criminal Law* 1, No. 2 (2020): 68-81.

hukum dalam melindungi pengguna kartu kredit dari berbagai bentuk kejahatan elektronik, terutama kejahatan yang berhubungan dengan aktivitas *cyber phising*, khususnya dalam kejahatan pencurian identitas kartu kredit.

DAFTAR PUSTAKA

Buku

Tim Indonesiabaik.id. *Tips Praktis di Dunia Siber* (Jakarta, Direktorat Jenderal Informasi dan Komunikasi Publik Kementerian Komunikasi dan Informatika, 2019).

Zam, Efvy. *Phising: Cara Mudah Menyadap Password dan Pencegahannya* (Jakarta, Mediakita, 2014).

Jurnal

Banjarnahor, Andrew Christian, and Puti Priyana. "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo." *Jurnal Hermeneutika* 6, No. 1 (2022): 32-36.

DM, Mohd. Yusuf., Vivi Yola, Destin Maiharani, and Egi Dwi. "Analisis Terhadap Modus-Modus Dalam Hukum *Cyber Crime*." *Jurnal Hukum, Politik dan Ilmu Sosial (JHPIS)* 1, No. 2 (2022): 64-70.

Fikri, Adi Wibowo Noor, Achmad Fauzi, Aldi Alfathur Rachman, dkk. "Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phising dalam Layanan Online Banking." *Jurnal Ilmu Multidisiplin* 2, No. 1 (2023): 84-91.

Gulo, Ardi Saputra, Sahuri Lasmadi, and Kabib Nawawi. "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik." *PAMPAS: Journal Of Criminal Law* 1, No. 2 (2020): 68-81.

Muftiadi, Amin, Tri Putri Mulyani Agustina, and Margaretha Evi. "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman *Phising* Terhadap Layanan *Online Banking*." *Jurnal Ilmiah Teknik* 1, No. 2 (2022): 60-65.

Rumlus, Muhamad Hasan, and Hanif Hartadi. "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik." *Jurnal HAM* 11, No. 2 (2020): 285-299.

Rustam. "Tinjauan Yuridis Terhadap Tindak Pidana Pencurian Kartu Kredit Dengan Menggunakan Internet di Indonesia." *Jurnal Trias Politika* 4, No. 2 (2020): 229-237.

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *Jurnal SASI* 27, No. 1 (2021): 38-52.

Wibowo, Mia Haryati, and Nur Fatimah. "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime." *Jurnal of Education and Information Communication Technology* 1, No. 1 (2017): 1-5.

Skripsi

H, Monica Shelsa. *Skripsi*: *Analisis Tindak Pidana Pencurian Data Pribadi Melalui Teknik Phising Ditinjau Dalam Perspektif Fiqih Jinayah* (Semarang, Fakultas Syariah dan Hukum Universitas Islam Negeri Walisongo, 2022), 52-53.

Website

Pusat Ensiklopedia. URL: https://p2k.stekom.ac.id/ensiklopedia/Pratama_Dahlian_Persadha#cite_note-14, diakses pada 7 Juli 2023.

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Lembaran Negara Republik Indonesia Nomor 75 Tahun 1959)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843)

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952)

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400)