Jurnal Ilmiah Wahana Pendidikan, Agustus 2025, 11(8.D), 232-244
DOI: https://jurnal.peneliti.net/index.php/JIWP/article/view/11224
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Penegakan Hukum Terhadap Modus Baru Kejahatan *Cyber* Berupa Rekayasa Informasi Teknologi Pembobolan Rekening Nasabah Melalui *Internet Banking*

Deya Hazirattul Khudsiyah[1], Davit Rahmadan[2], Erdianto[3]

[1,2,3] Universitas Riau

Received: 07 July 2025
Revised: 16 July 2025
Accepted: 23 July 2025

Abstract

Electronic transaction dalam bentuk internet banking merupakan bentuk baru pengembangan layanan bank untuk dalam rangka berperan sebagai penghubung kebutuhan dunia usaha dan nasabah dalam hal mempercepat pelayanan jasa bank. Kemudahan yang diberikan oleh kemunculan electronic banking, berbanding lurus dengan bahaya yang mengintainya. Potensi kebocoran informasi pribadi yang dilakukan oleh peretas, menjadi bayang- bayang buruk nasabah bank sebagai pengguna electronic banking. Hal ini didukung dengan modus operandi kejahatan di dunia perbankan berkembang dan makin canggih, terutama dengan pemanfaatan teknologi informasi. Jenis penelitian ini tergolong sebagai penelitian hukum Sosiologis yang membahas tentang Pengaruh berlakunya hukum positif terhadap kehidupan masyarakat, sedangkan dilihat dari sifatnya penelitian tersebut bersifat deskriptif yaitu suatu penelitian yang dimaksudkan untuk memberikan data yang seteliti mungkin dengan manusia, keadaan atau gejala-gejala lainnya, serta hanya menjelaskan keadaan objek masalahnya tanpa bermaksud mengambil kesimpulan yang berlaku umum. Berdasarkan hasil penelitian dan pembahasan dapat disimpulkan. Pertama Modus Kejahatan Cyber dalam Internet Banking Seiring dengan perkembangan teknologi informasi, modus kejahatan cyber terus mengalami transformasi. Salah satu bentuk kejahatan cyber yang meresahkan adalah rekayasa informasi teknologi, di mana pelaku kejahatan menggunakan metode teknis untuk membobol rekening nasabah melalui internet banking. Kedua Bank telah memberikan perlindungan kepada nasabah dari tindakan phishing, pharming dan spoofing melalui 2 (dua) cara, yaitu cara preventif dan represif. Perlindungan preventif yang diberikan oleh Bank berupa edukasi melalui platform media sosial resmi Bank, dan Ketiga Dalam konteks kejahatan cyber, tantangan terbesar adalah penegakan hukum yang efektif, mengingat karakteristik kejahatan ini bersifat lintas batas, canggih, dan terus berkembang. Oleh karena itu, harus beradaptasi dengan tantangan era digital.

Keywords: *Penegakan Hukum Kejahatan Cyber,Pembobolan Rekening, Nasabah, Internet Banking*

(*) Corresponding Author: deyahazirattul10@gmail.com
davit.rahmadan@lecturer.unri.ac.id ,
erdianto.effendi@lecturer.unri.ac.id

How to Cite: Khudsiyah, D., Rahmadan, D., & Erdianto, E. (2025). Penegakan Hukum Terhadap Modus Baru Kejahatan Cyber Berupa Rekayasa Informasi Teknologi Pembobolan Rekening Nasabah Melalui Internet Banking. *Jurnal Ilmiah Wahana Pendidikan*, *11*(8.D), 232-244. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/11224.

INTRODUCTION

Pesatnya pembangunan dan perkembangan perekonomian nasional telah menghasilkan variasi produk barang atau jasa yang dapat di konsumsi. Kemajuan di bidang ilmu pengetahuan dan teknologi telekomunikasi dan informatika juga turut

mendukung perluasan ruang gerak transaksi barang atau jasa hingga melintasi batasbatas wilayah suatu negara.

Dalam kehidupan sehari-hari bentuk transaksi menggunakan teknologi ini dapat dilihat dalam wujud *electronic transaction* (*e-banking*) melalui ATM, *phone banking*, *internet banking* dan lain sebagainya sebagai bentuk baru delivery channel (saluran pengiriman) memoderenisasi setiap transaksi. Secara umum saat ini setidaknya terdapat tiga basis instrument pembayaran, Seperti *: Papper-based* yaitu (*cek, bilyet giro* dan *nota debet*), *Card- based* yaitu (kartu kredit,kartu debet dan kartu ATM), *Electronic-based* yaitu (*emoney, internet banking, mobile banking, electronic mall*).[1]

Menurut survei Asosiasi Bankir Indonesia (ABI) pada tahun 2020, jumlah pengguna internet banking di Indonesia mencapai 73,6 juta orang. Sementara itu Bank Indonesia menunjukkan bahwa pada kuartal II 2021, jumlah transaksi menggunakan internet banking di Indonesia mencapai 1,5 miliar transaksi.mpengguna internet banking di Indonesia pada kuartal II 2021 mengalami peningkatan sebesar 0,87% dibandingkan kuartal sebelumnya. Bank-bank terbesar di Indonesia, seperti Bank Mandiri, Bank Central Asia (BCA), dan Bank Rakyat Indonesia (BRI), menyatakan bahwa penggunaan internet banking meningkat signifikan pada tahun 2020-2022.[2]

Tingginya pengguna internet di indonesia dalam hal ini Bank Indonesia sebagai regulator dan pengawas kegiatan perbankan di Indonesia mengeluarkan Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Pada Bank Umum, agar setiap bank yang menggunakan teknologi informasi khususnya *Internet banking*, dapat meminimalisir risiko-risiko yang timbul sehubungan dengan kegiatan tersebut sehingga mendapatkan manfaat yang maksimal dari penggunaan teknologi informasi. Layanan yang diberikan kepada nasabah berupa transaksi pembayaran tagihan, informasi rekening, pemindah bukuan antar rekening, infomasi terbaru mengenai suku bunga dan nilai tukar *valuta asing*, administrasi mengenai perubahan Personal Identification Number (PIN), alamat rekening atau kartu, data pribadi dan lain-lain, terkecuali pengambilan uang atau penyetoran uang.[3]

Saat ini sedang berkembang kejahatan *Cyber* Berupa Rekayasa Informasi Teknologi Pembobolan Rekening Nasabah Melalui *Internet Banking* Modus-modus pembobolan rekening ini seperti:[4]

1. Mengirimkan link penggantian kartu ATM untuk mencuri data pribadi.
2. Mengirimkan undangan pernikahan digital palsu.
3. Mengatasnamakan perusahaan listrik dengan modus pembayaran tagihan.
4. Mengirimkan pengumuman bantuan subsidi upah BPJS.

Pembobolan rekening bank melalui rekayasa sosial (*social engineering*) yakni dengan memanfaatkan pergantian SIM Card baru atau data nasabah menjadi modus kejahatan baru di Indonesia yang dinilai sangat berbahaya. Contohnya, kasus pembobolan yang menimpa wartawan senior yang menghebohkan belakangan ini. Si pelaku diketahui

[1] Umul Khair, Anny Yuserlina, Perlindungan Hukum Data Nasabah Internet Banking Di Bri Kota Bukittinggi Dan Payakumbuh, *Jurnal ensikopediaku Lembaga Penelitian dan Penerbitan Hasil Penelitian Ensiklopedia*, Vol. 1 No.2 Juni 2019 Sekolah Tinggi Ilmu Hukum Putri Maharaja Payakumbuh, hal 235.

[2] https://databoks.katadata.co.id/datapublish/2021/10/07/pengguna-bank-digital-di-indonesia-diproyeksi-capai-748-juta-pada-2026, di akses tanggal 6 Mei 2023 Jam 14.05.

[3] Muhammad Yakup, Abdul Gani, Emil Salim Siregar, Pengaturan Hukum Terhadap Layanan Internet Banking Dalam Transaksi Perbankan, *Jurnal Pionir LPPM Universitas Asahan Vol. 6 No. 1 Januari 2020, Program Studi Ilmu Hukum*, Fakultas Hukum, Universitas Asahan, Kisaran, hal 32.

[4] https://www.solopos.com/waspada-kenali-modus-baru-pembobolan-rekening-bank-dan-cara-mencegahnya-1537548 diakases tanggal 22 Febaruari 2023 jam 11.36 Wib.

melakukan rekayasa sosial yang diawali dengan memanfaatkan data dari Sistem Layanan Informasi Keuangan (SLIK) yang ada di Otoritas Jasa Keuangan (OJK) yang ia beli dari pegawai bank.[5]

Kasus lain yaitu pembobolan *e-banking* yang dilakukan oleh dua orang yang menguras Rp 1,12 miliar dana korban. Awalnya korban melapor ke Polisi kehilangan uang melalui m-banking padahal transaksi tak pernah gunakan *Mobile Banking*. Usut punya usut, ternyata pelaku kejahatan pelaku kejahatan menggunakan kartu perdana korban yang sudah mati yang sebelumnya digunakan untuk aktivasi *Mobile Banking*. Kartu perdana tersebut dihidupkan kembali dan digunakan untuk bertransaksi. Tidak hanya itu kasus Pembobolan dana nasabah melalui internet banking atau *Mobile Banking* dengan menguasai nomor ponsel korban modus yang sering dilakukan beberapa penjahat di Indonesia

Maraknya kasus pembobolan Rekening nasabah melalui internet banking harus adanya penegakan hukum, saat ini penegakan hukum terhadap kejahatan *Cyber* terkait dengan pembobolan rekening nasabah masih sulit karena sulinya menjangkau pelaku kejahatan apalagi pelaku yang berada di luar negeri, selain itu bank juga tidak bertanggung jawab atas kehilangan dana nasabah sedang dalam hal ini bank wajib melindungan nasabah, perlunya penegakan hukum terhadap kejahatan ini agar memberikan keadilan bagi nasabah sehingga tidak ada lagi nasabah bank yang menjadi korban apalagi kerungian yang di dapat nasabah tersebut mencapai ratusan juta rupiah bahkan milyaran rupiah.

Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik sebagai payung hukum dalam Kejahatan *Cyber* masih memiliki kelemahan dalam penegakan hukum yang mana belum mengatur secara khusus tentang kejahatan *cyber* di sektor perbankan, sehingga sulit untuk menjerat pelaku yang melakukan pembobolan rekening nasabah melalui *internet banking* dengan pasal-pasal yang ada di Undang-Undang Informasi dan Transaksi Elektronik.[6]

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik juga belum mengatur secara jelas tentang tanggung jawab bank sebagai penyedia layanan *internet banking* terhadap nasabah yang menjadi korban pembobolan rekening. Apakah bank harus memberikan ganti rugi, kompensasi, atau penggantian kepada nasabah, dan bagaimana mekanisme dan prosedurnya.[7]

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik belum mengatur secara tegas tentang sanksi pidana dan perdata bagi pelaku kejahatan *cyber* di sektor perbankan, sehingga tidak memberikan efek jera dan pencegahan terhadap kejahatan *cyber* yang semakin marak. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik juga belum mengatur secara komprehensif tentang kerjasama antara pihak-pihak yang terkait dalam penanganan kejahatan *cyber* di sektor perbankan, seperti antara bank, nasabah, kepolisian, kejaksaan, pengadilan, dan lembaga-lembaga lainnya. Hal ini menyebabkan adanya kesulitan dalam koordinasi, penyelidikan, penyidikan, penuntutan, dan penyelesaian perkara.[8]

[5] https://www.cnbcindonesia.com/tech/20200207183932-37-136254/tips-dari-ojk-agar-terhindar-kasus-pembobolan-rekening-bank diakases tanggal 22 Febaruari 2023 jam 11.36 Wib

[6] https://www.hukumonline.com/klinik/a/tanggung-jawab-bank-atas-pembobolan-rekening-nasabah-lt5ea6e27adf366, diakases tanggal 3 November 2023, Jam 19.00 Wib.

[7] Purnomo, Kebijakan Hukum Terhadap Kejahatan Cybercrime Di Era Informasi Dan Masyarakat Virtual, *Jurnal Palimpsest*, Tahun IX, Nomor 2, Desember 2017-Mei 2018, hlm.79

[8] https://finansial.bisnis.com/read/20211111/90/1464684/pahami-jenis-jenis-kejahatan-siber-di-sektor-perbankan diakases tanggal 3 November 2023, Jam 19.00 Wib.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik juga belum mengatur secara spesifik tentang teknik-teknik dan metode-metode yang digunakan oleh pelaku kejahatan *cyber* di sektor perbankan, seperti *skimming, phishing, malware, hacking*, dan lain-lain. Hal ini menyebabkan adanya kesenjangan antara perkembangan teknologi informasi dan hukum yang mengaturnya.[9]

METHODS

Jenis penelitian ini tergolong sebagai penelitian hukum Sosiologis. Adapun yang menjadi populasi penelitian ini adalah Penyidik Kepolisian Daerah Riau, Direktur Reskrimsus Polda Riau, dan Korban Tindak Pidana. Dalam menentukan sampel penulis menggunakan teknik *purposive sampling.* Tidak semua populasi yang dijadikan sampel. Sampel dari penelitian ini diambil dari organ-organ yang terdapat pada populasi yang ada di Kepolisian Daerah Riau. Metode pengumpulan data yang digunakan dalam penelitian ini adalah wawancara dan kajian kepustakaan. Penelitian ini analisis data yang digunakan adalah analisis secara kualitatif yaitu uraian yang dilakukan peneliti terhadap data yang terkumpul tidak menggunakan statistik atau matematika ataupun sejenisnya, tetapi berupa uraian-uraian kalimat yang tersusun secara sistematis sesuai dengan permasalahan yang dibahas. Dalam menarik kesimpulan penulis menggunakan metode berfikir deduktif yaitu cara berfikir yang menarik kesimpulan dari suatu pernyataan atau dalil yang bersifat umum menjadi suatu pernyataan yang bersifat khusus.

RESULTS & DISCUSSION

1. Modus Baru Kejahatan *Cyber* Berupa Rekayasa Informasi Teknologi dengan Membobol Rekening Nasabah Melalui *Internet Banking*

Belakangan ini fenomena kejahatan perbankan yang berhubungan erat dengan penggunaan teknologi berbasis komputer dan jaringan internet semakin marak. Salah satunya adalah pembobolan rekening nasabah melalui fasilitas *internet banking*. Adapun pembobolan *internet banking* yang marak dilakukan antara lain:

1. *Modus Phising*

Kegiatan *Phishing* adalah kegiatan untuk mengelabui penerima *e-mail* untuk mendapatkan informasi yang diinginkan oleh pengirim, caranya sama seperti melakukan *Spamming* (mengirimkan *e-mail* tetapi tidak mengenal siapa yang akan menerima) tetapi memiliki tujuan lebih khusus lagi,[10] misalnya nomor *credit card*, alamat, nomor *personal identification number* (PIN), *password e-mail* dan lain sebagainya. Cara penipuan dengan modus *phishing* sangat beragam, dari sekedar meminta penerima *e-mail* memasukan informasi tertentu, dengan mengatakan ini diperlukan sebagai *update* atau dengan mengatakan penerima *e-mail* telah mendapat hadiah, dan meminta penerima *e-mail* mengirimkan identifikasi pribadi dan lainnya. [11]

Definisi phishing adalah tindakan penipuan yang menggunakan e-mail palsu atau situs web palsu yang bertujuan untuk mengelabui user sehingga pelaku bisa mendapatkan data user tersebut.[12] Tindakan phishing diidentifikasikan sebagai proses untuk menarik orang untuk mengunjungi situs web palsu yang dibuat serupa seperti yang asli dan

[9] https://nasional.kompas.com/read/2022/09/16/02400071/kejahatan-siber--pengertian-karakteristik-dan-faktor-penyebabnya diakases tanggal 3 November 2023, Jam 19.30 Wib.

[10] http://root.wanxp.netindex.phpoption, diakses pada tanggal 20 Februari 2024. Jam 19.00.

[11] *Ibid*

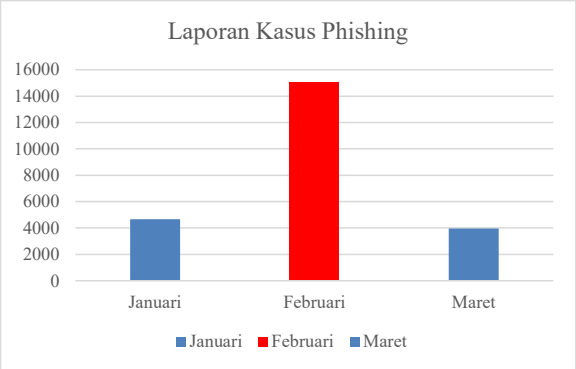
[12] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*, CV Andi Offset, Yogyakarta:, 2013, hlm. 214.

Formatted: Font: 12 pt, Bold
Formatted: Font: Italic
Formatted: Font: 12 pt, Bold
Formatted: Font: 12 pt, Bold, Italic
Formatted: Font: 12 pt, Bold
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: 12 pt, Italic
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, Italic
Formatted: Font: Times New Roman
Formatted: Justified, Indent: First line: 0,75 cm
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, English (United States)

mengakibatkan mereka memasukkan informasi mengenai identitas pribadi seperti nama pengguna, kata sandi, nomor Personal Identification Number (PIN). [13]

Phishing yaitu aktivitas seseorang untuk mendapatkan informasi rahasia *user* dengan cara menggunakan *e-mail* dan situs *web* yang menyerupai aslinya atau resmi. Informasi rahasia yang diminta biasanya berupa *password account* atau nomor kartu kredit, detail pembayaran dan sebagainya. *Password* adalah sebuah kode rahasia yang biasanya digunakan untuk menjalankan proses autentifikasi yakni sebuah proses untuk melakukan konfirmasi apakah seseorang memiliki izin untuk mengakses informasi atau data yang dirahasiakan. *Password* sendiri selalu dijadikan sebuah rahasia yang hanya diketahui oleh individu atau kelompok yang memiliki hak untuk mengakses data atau informasi yang dilindungi tersebut.[14]

Gambar 3.1 Laporan Kasus Phishing di Indonesia



Sumber: Indonesia Anti-Phishing Data Exchange (IDADX)

2. *Pharming*

Pharming adalah gabungan kata dari *phising* dan *farming* yang merupakan suatu jenis serangan siber dimana penjahat mengarahkan pengguna internet yang ingin mengunjungi suatu website namun dialihkan ke situs web palsu yang berbeda. Adapun tujuan dari kejahatan ini adalah untuk mendapatkan informasi pribadi pengguna dan mengidentifikasi login credentials seperti password, nomor akun, nomor keamanan sosial, dan sebagainya.

Adapun yang membuat *pharming* berbahaya dibandingkan dengan kejahatan lainnya karena *pharming* hanya memerlukan aksi yang sedikit dari pengguna. Layaknya pada kasus DNS Poisoning pengguna yang terpengaruh dapat saja memiliki komputer yang sepenuhnya bebas malware namun tetap bisa menjadi korban.

Bahkan mengambil tindakan pencegahan seperti memasukkan alamat situs web secara manual pun atau selalu menggunakan bookmark terpercaya juga tidak cukup, karena penyesatan terjadi setelah komputer mengirimkan permintaan koneksi. Salah satu cara terbaik untuk terlindungi dari serangan phising adalah melakukan install atau menjalankan software anti-virus atau anti-malware dari provider terpercaya.

3. *Spoofing*

[13] T. Moore and R. Clayton, An empirical analysis of the current state of phishing attack and defence", *In Proceedings of the Sixth Workshop on the Economics of Information Security*, Vol. 4 No. 3, 2007, hlm 1.

[14] Thor, Zero, *Knowledge Password*, PT Elex Media Komputindo Gramedia Kelompok Gramedia, Jakarta, 2008, hlm. 2.

Formatted: Font: 12 pt
Formatted: Font: 12 pt, Swedish (Sweden)
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: Italic
Formatted: Font: 12 pt, Italic
Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 0,75 cm, Numbered + Level: 4 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 4,81 cm + Indent at: 5,44 cm
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: 12 pt
Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 0,75 cm, Numbered + Level: 4 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 4,81 cm + Indent at: 5,44 cm
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, Italic
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, English (United States)

Spoofing adalah bentuk kejahatan siber dengan praktik penyamaran informasi yang dalam praktiknya pelaku seakan-akan berperan sebagai pihak berwenang, seperti dari bank atau institusi lainnya, untuk memperoleh akses secara tidak sah ke suatu komputer, telepon seluler atau handphone, email, maupun sistem informasi. *Spoofing* biasanya menampilkan alat email/nama/nomor telepon palsu di komputer untuk menyembunyikan identitas asli mereka, hal ini juga untuk memberikan kesan bahwa korban sedang berurusan dengan perusahaan, institusi, atau lembaga resmi.
Tujuan pelaku *spoofing* yaitu untuk mendapatkan informasi sensitif seperti informasi pribadi maupun informasi organisasi yang hingga bisa menimbulkan kerugian materi dari korbannya.

Data diatas didukung oleh hasil wawancara peneliti dengan Penyidik Kepolisian Daerah Riau, beliau menyatakan:
"Sejauh ini kasus *internet banking* di daerah Polda Riau ada beberapa kasus telah terjadi, diantara kasus yang ada itu berupa *phishing,* kasus ini biasanya pelaku lakukan dengan pemberian hadiah, maupun memberikan informasi palsu kepada korban".

Jika di kaitkan dengan Teori Kepastian Hukum, Teori ini menekankan bahwa hukum harus jelas, tegas, konsisten, dan dapat diprediksi sehingga masyarakat dapat mengatur perilaku mereka sesuai dengan aturan yang berlaku. Kepastian hukum memberikan perlindungan terhadap hak-hak individu dan memastikan bahwa tindakan yang melanggar hukum akan dikenakan sanksi. Dalam konteks kepastian hukum, negara berkewajiban menjamin bahwa setiap pelanggaran hukum dapat diadili dengan adil dan tepat waktu, serta masyarakat memiliki kepercayaan pada sistem peradilan.

Kemudian Modus Kejahatan Cyber dalam Internet Banking Seiring dengan perkembangan teknologi informasi, modus kejahatan cyber terus mengalami transformasi. Salah satu bentuk kejahatan cyber yang meresahkan adalah rekayasa informasi teknologi, di mana pelaku kejahatan menggunakan metode teknis untuk membobol rekening nasabah melalui internet banking. Teknik yang digunakan bervariasi, mulai dari phishing, malware, hingga peretasan melalui kerentanan sistem. Tujuan utama para pelaku adalah mencuri informasi pribadi, seperti kata sandi dan kode otentikasi, untuk mendapatkan akses ke rekening nasabah dan mencuri dana. Modus ini semakin sulit dideteksi dan diberantas karena para pelaku terus memperbarui teknik mereka sesuai dengan kemajuan teknologi. Kejahatan seperti ini sering kali melibatkan jaringan internasional, yang memperumit upaya penegakan hukum.

2. Upaya Pihak Bank untuk mengatasi kejahatan *cyber* berupa rekayasa informasi teknologi dengan membobol rekening nasabah melalui *internet banking*

Pada penelitian ini peneliti mengambil data pada PT Bank Rakyat Indonesia (Persero) Tbk di Pekanbaru atau yang biasa dikenal dengan nama Bank BRI merupakan salah satu bank terbesar di Indonesia, yang memiliki lebih dari 100 juta nasabah. [15] Nasabah berdasarkan Pasal 1 Butir 16 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang - Undang Nomor 7 Tahun 1992 tentang Perbankan, didefinisikan sebagai pihak yang menggunakan jasa bank. Kepercayaan nasabah kepada Bank BRI merupakan hal yang sangat penting. Akan tetapi berbagai kejahatan dalam dunia perbankan yang mengancam keamanan simpanan nasabah menjadi duri tajam dalam menjaga reputasi dan kepercayaan nasabah kepada Bank BRI, salah satunya adalah tindakan *phishing* *pharming,* dan *spoofing*.

Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Indent: Left: 0 cm, First line: 1,27 cm
Formatted: Font: 12 pt, Bold
Formatted: Font: 12 pt, Bold
Formatted: Font: 12 pt, Bold
Formatted: Font: 12 pt, Bold
Formatted: Font: 12 pt, Bold
Formatted: Font: 12 pt, Bold
Formatted: Font: 12 pt, Bold

Tanggung jawab bank terhadap perlindungan nasabah terdapat dalam aturan di bidang sektor jasa keuangan. Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum mengatur juga tentang perlindungan nasabah, dimana Peraturan OJK ini menyebutkan, bank penyelenggara layanan perbankan digital wajib menerapkan prinsip perlindungan konsumen sebagaimana dimaksud dalam ketentuan peraturan perundang-undangan.

Prinsip perlindungan nasabah menurut Pasal 2 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan mencakup transparansi, perlakuan yang adil, keandalan, kerahasiaan serta keamanan data/informasi nasabah dan penanganan pengaduan serta penyelesaian sengketa nasabah secara sederhana, cepat dan biaya terjangkau. Perlindungan nasabah dari tindakan phishing merupakan bentuk tanggung jawab bank kepada nasabah yang mengalami kerugian. Perlindungan terhadap nasabah bank didasarkan oleh bentuk hubungan antara bank dengan nasabah, yaitu hukum dan kepercayaan.[16] Bank dalam melakukan kegiatannya harus mematuhi prinsip-prinsip pengelolaan bank, yaitu prinsip kepercayaan (*fiduciary principle*), prinsip kehati-hatian (*Prudential principle*), prinsip kerahasiaan (*confidential principle*), dan prinsip mengenal nasabah (*know your customer principle*).[17]

Perlindungan nasabah secara preventif tercantum dalam Pasal 4 Undang-Undang perlindungan konsumen, yang menyatakan bahwa bank memiliki kewajiban untuk memberikan pembinaan dan pendidikan bagi nasabah sebagai konsumen. Selain itu hal selaras juga diatur dalam Pasal 9 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, bahwa Pelaku Usaha Jasa Keuangan wajib memberikan pemahaman kepada Konsumen mengenai hak dan kewajiban Konsumen.

Dalam menjalankan kegiatan operasionalnya, kegiatan perbankan selalu diikuti oleh risiko. Risiko dalam POJK Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum merupakan potensi kerugian akibat terjadinya suatu peristiwa tertentu. Menurut The Office The Comptroller of the currency (OCC) ditemukan beberapa kategori risiko yang ada dalam penyelenggaraan layanan internet banking, yaitu sebagai berikut: (a) Risiko kredit (*credit risk*); (b) Risiko suku bunga (*interest rate risk*); (c) Risiko likuiditas (*liquidity risk*); (d) Risiko transaksi (*transaction risk*); (e) Risiko komplain (*complience risk*); (f) Risiko reputasi (*reputation risk*).

Dengan adanya potensi terjadi risiko ini maka bank wajib melakukan manajemen risiko untuk mengurangi potensi terjadinya risiko yang akan merugikan nasabah. Kewajiban bank untuk melakukan manajemen risiko tercantum dalam Pasal 2 POJK Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum. Menurut aturan a quo, penerapan manajemen risiko paling sedikit harus mencakup:

1) Pengawasan aktif direksi dan dewan komisaris
2) Kecukupan kebijakan dan prosedur manajemen risiko serta pengendalian limit risiko
3) Kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko, serta sistem informasi manajemen risiko
~~1)~~4) Sistem pengendalian intern yang menyeluruh

Berdasarkan Pasal 29 POJK Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Dalam penggunaan Teknologi Informasi Oleh Bank Umum,

[16] Ronny Sautama Hotma Bako, *Hubungan Bank Dengan Nasabah Terhadap Produk Tabungan Dan Deposito*, Citra Aditya Bakti, Bandung, 1995, hlm. 32.

[17] Rachmadi Usman, 2003, *Aspek-aspek Hukum Perbankan Indonesia*, Gramedia Pustaka, Jakarta, 2003, hlm.19.

Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: 12 pt
Formatted: List Paragraph, Indent: Left: 0 cm, Line spacing: single, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,63 cm + Indent at: 1,27 cm
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: List Paragraph, Indent: Left: 0 cm, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,63 cm + Indent at: 1,27 cm
Formatted: Font: 12 pt
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, Italic
Formatted: Justified, Indent: First line: 0,75 cm
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, English (United States)
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, Italic
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, English (United States)

menyatakan bahwa bank wajib menerapkan prinsip pengendalian pengamanan data nasabah dan transaksi layanan perbankan elektronik pada setiap sistem elektronik yang digunakan oleh bank. Selain itu Dalam Pasal 15 ayat (1) dan (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang nomor 11 Tahun 2008 Tentang informasi dan Transaksi Elektronik mewajibkan setiap penyelenggara sistem elektronik untuk menyediakan sistem elektronik secara andal dan aman, dan bertanggung jawab untuk memastikan sistem elektronik berjalan sebagaimana mestinya. Secara lebih lanjut dijelaskan dalam penjelasan undang-undang a quo. kata "Andal" artinya sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunanya. "Aman" artinya sistem elektronik terlindungi secara fisik maupun non-fisik. "Beroperasi sebagaimana mestinya" artinya sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya. "Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut.

Bank dalam hal ini wajib melakukan pelaporan kondisi terkini penggunaan Teknologi Informasi paling lambat 1 (satu) bulan sejak akhir tahun pelaporan. Kemudian bank juga wajib melaporkan rencana pengembangan teknologi informasi yang akan diimplementasikan 1 (satu) tahun ke depan paling lambat 31 Oktober tahun sebelumnya.

Kemudian terdapat perlindungan terhadap nasabah atas keadaan yang tidak diinginkan diatas yang telah terjadi serta merugikan nasabah, sehingga perlu adanya upaya dalam menyelesaikan permasalahan tersebut. Perlindungan yang tujuannya menyelesaikan masalah atau sengketa yang timbul dikenal dengan perlindungan represif. Perlindungan represif diberikan ketika perlindungan secara preventif tidak dapat menghindarkan nasabah dari tindakan *phishing*, *fharming* dan *spoofing*. Dalam Pasal 4 huruf d Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan konsumen, konsumen mempunyai hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan. Kemudian selain itu dalam Pasal 32 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan menyatakan bahwa Pelaku usaha jasa keuangan wajib memiliki dan melaksanakan mekanisme pelayanan dan penyelesaian bagi konsumen.

Dalam menangani dan menyelesaikan pengaduan yang diajukan konsumen, maka bank diwajibkan untuk memiliki unit kerja dan/atau fungsi untuk menangani dan menyelesaikan pengaduan yang diajukan konsumen. Ketentuan ini terdapat dalam Pasal 36 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Setelah menerima pengaduan konsumen, maka pihak bank wajib untuk melakukan:

a. Pemeriksaan internal atas pengaduan secara kompeten, benar, dan obyektif;
b. Melakukan analisis untuk memastikan kebenaran pengaduan;
c. menyampaikan pernyataan maaf dan menawarkan ganti rugi (*redress/remedy*) atau perbaikan produk dan atau layanan, jika pengaduan nasabah benar.

Berdasarkan Pasal 7 huruf f Undang-Undang Perlindungan konsumen, bank sebagai pelaku usaha wajib memberikan ganti rugi kepada nasabah sebagai konsumen akibat penggunaan, pemakaian dan pemanfaatan barang dan/atau jasa yang diperdagangkan. Kewajiban pemberian ganti rugi oleh bank juga tercantum dalam Pasal 38 huruf c POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yaitu bank memiliki kewajiban untuk menyampaikan permintaan maaf dan menawarkan ganti rugi (*redress/remedy*) atau perbaikan produk dan/atau layanan, jika pengaduan konsumen benar dan Pasal 29 Undang-Undang *a quo*, bahwa menyatakan

Formatted: Font: Italic

Formatted: Font: 12 pt

Formatted: List Paragraph, Indent: Left: 0 cm, Line spacing: single, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0,63 cm + Indent at: 1,27 cm

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Font: 12 pt, Italic

Formatted: Font: 12 pt

Formatted: Font: Italic

Formatted: Font: Italic

pelaku usaha jasa keuangan wajib bertanggung jawab atas kerugian konsumen yang timbul akibat kesalahan dan/atau kelalaian, pengurus, pegawai pelaku usaha jasa keuangan dan/atau pihak ketiga yang bekerja untuk kepentingan pelaku usaha jasa keuangan. Namun pemberian ganti rugi tersebut tidak berlaku apabila bank dapat membuktikan bahwa terjadinya phishing merupakan kesalahan dan kelalaian dari pihak nasabah sendiri, sesuai dengan ketentuan dalam Pasal 21 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Apabila nasabah merasa tidak mencapai kesepakatan penyelesaian pengaduan, maka berdasarkan ketentuan dalam Pasal 39 POJK Perlindungan Konsumen Sektor Jasa Keuangan, nasabah dapat melakukan penyelesaian sengketa di pengadilan maupun di luar pengadilan. Selain itu nasabah juga dapat menyampaikan pengaduan yang berindikasi sengketa antara bank dan nasabah kepada Otoritas Jasa Keuangan (OJK) yang diakibatkan adanya indikasi pelanggaran atas ketentuan peraturan perundang-undangan di dalam bank, sebagaimana dalam Pasal 40 POJK Perlindungan Konsumen Sektor Jasa Keuangan.

Berdasarakan Analisi Penulis dengan Teori pemidanaan dalam upaya pihak bank untuk mengatasi kejahatan cyber berupa rekayasa teknologi informasi dengan membobol rekening nasabah melalui internet banking dapat dianalisis secara lebih mendalam melalui pendekatan teori retributif, teori utilitarian, dan teori rehabilitatif. Ketiganya memberikan perspektif yang komprehensif untuk memahami tujuan pemidanaan sekaligus peran bank dalam melindungi nasabahnya di era digital yang penuh risiko.

Dari sudut pandang teori retributif, kejahatan cyber seperti pembobolan rekening nasabah merupakan pelanggaran serius yang merugikan korban secara materiil dan moral. Hukuman yang dijatuhkan kepada pelaku harus mencerminkan tingkat kesalahan mereka, termasuk dampak kerugian yang dihasilkan. Dalam hal ini, hukuman berat, seperti pidana penjara yang lama, denda maksimal, atau penyitaan aset yang diperoleh dari hasil kejahatan, dapat dilihat sebagai upaya memberikan rasa keadilan kepada korban. Teori ini juga mendukung prinsip bahwa setiap pelanggaran hukum harus direspons dengan hukuman yang setimpal untuk menjaga otoritas hukum dan keadilan sosial.

Selanjutnya, teori utilitarian menekankan tujuan pemidanaan sebagai upaya untuk mencegah kejahatan serupa di masa depan. Efek jera (deterrence) menjadi kunci dalam teori ini. Hukuman yang berat dan dipublikasikan dengan baik dapat memberikan peringatan kepada masyarakat dan calon pelaku lainnya agar tidak mencoba melakukan tindakan serupa. Bank juga berperan dalam mendukung aspek pencegahan ini melalui penguatan sistem keamanan teknologi, seperti implementasi dua faktor autentikasi (2FA), enkripsi data tingkat tinggi, dan deteksi aktivitas mencurigakan secara real-time. Selain itu, bank dapat bekerja sama dengan pihak berwenang untuk meningkatkan kapasitas penegak hukum dalam melacak dan menangkap pelaku kejahatan cyber, termasuk melalui pelatihan teknis atau pembentukan tim investigasi khusus.

Teori rehabilitatif, di sisi lain, menganggap bahwa pelaku kejahatan cyber, meskipun telah melakukan pelanggaran hukum, tetap memiliki potensi untuk berubah. Mengingat keahlian teknologi yang sering dimiliki pelaku kejahatan semacam ini, rehabilitasi dapat diarahkan pada pengalihan keterampilan mereka ke bidang yang legal dan produktif, seperti pengembangan perangkat lunak atau keamanan siber. Program rehabilitasi yang baik dapat mengurangi kemungkinan residivisme, yaitu pelaku kembali melakukan kejahatan setelah menjalani hukuman. Dalam konteks ini, bank juga dapat memainkan peran dengan menyediakan program kemitraan, misalnya mendukung pelaku

yang telah direhabilitasi untuk menjadi konsultan keamanan atau bagian dari upaya memperkuat sistem teknologi informasi perbankan.

3. Penegakan hukum terhadap modus baru Kejahatan *Cyber* berupa rekayasa informasi teknologi dengan membobol rekening Nasabah Melalui *Internet Banking*

Di Indonesia, penegakan hukum terhadap kejahatan dunia maya di bidang perbankan diatur dengan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Elektronik dan Hukum Digital. Khususnya pada pasal 27 sampai 30 mengenai perbuatan yang dilarang. Lebih lanjut, aturan tentang hacking diatur dalam pasal 30 ayat 1, 2, dan 3. Sanksi pidana bagi yang melanggar ketentuan pasal 30 UU ITE diatur di dalam pasal 46 UU ITE berupa. 6-8 tahun penjara dan denda Rp600.000.000,00- Rp800.000.000,00.

Ketentuan penyidikan dalam UU ITE berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan. Selain UU ITE, peraturan yang landasan dalam penanganan kasus cyber crime di Indonesia ialah peraturan pelaksana UU ITE dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.

Secara sosiologis, masyarakat memang membutuhkan suatu peraturan tentang regulasi hukum yang konkrit tentang teknologi informasi yang sebelum dikeluarkannya UU ITE, peraturan yang ada hanya sebatas berhubungan dengan teknologi informasi, belum menjelaskan dengan secara langsung dan lebih konkrit. Dengan adanya UU ITE dimaksudkan untuk mengatur berbagai aktivitas masyarakat saat berinteraksi di cyber space.

Selain memenuhi syarat sosiologis, UU ITE juga telah memenuhi syarat secara filosofis. Secara filosofis, lahirnya UU ITE ini didasarkan pada amanat yang terkandung dalam Pasal 28F Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan " Setiap orang berhak untuk mencari, memperoleh, memiliki, meyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia".

Tindakan-tindakan kejahatan *cyber* / *cyber crime* yang dimuat dalam Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu, sebagai berikut : 1)Tindakan yang melanggar kesusilaan Dalam Pasal 27 ayat (1) UU Nomor 11 Tahun 2008 disebutkan "Setiap orang dengan sengaja dan tanpa hak mendistribusikan danatau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan", tetapi dalam pasal tersebut tidak dijelaskan mengenai perbuatan yang memiliki muatan yang melanggar kesusilaan.[18]

Karakteristik hukum kejahatan dunia maya (cybercrime) yang bersifat ultimum remedium mengacu pada prinsip bahwa hukum pidana seharusnya menjadi upaya terakhir (the last resort) dalam menyelesaikan suatu permasalahan hukum, termasuk dalam konteks kejahatan siber. Pendekatan ini didasarkan pada pertimbangan bahwa sanksi

[18] Mudadi & Barda Nawawi, *Teori-teori dan Kebijakan Pidana*, PT. Alumni Bandung, 2010, hlm. 157.

Formatted: Font: 12 pt, Bold

Formatted: Font: Italic

pidana memiliki dampak yang signifikan terhadap pelaku, baik secara fisik, psikologis, maupun sosial, sehingga penerapannya harus dilakukan secara hati-hati dan hanya jika cara-cara lain tidak memadai untuk melindungi kepentingan hukum yang dilanggar. Dalam kasus cybercrime, sifat ultimum remedium ini memiliki beberapa karakteristik yang penting untuk dipahami.

Sedangkan terdapat beberapa upaya pencegahan tindak pidana, ataupun penanganan tindak pidana dimana UU ITE yang menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan computer (*cybercrime*), termasuk kejahatan pencurian data kartu kredit, pencucian uang dan kejahatan terorisme, yaitu antara lain:

1. Pertama, terkait tanggung jawab penyelenggara sistem elektronik, perlu dilakukan pembatasan atau limitasi atas tanggungjawab sehingga tanggungjawab penyelenggara tidak melampaui kewajaran.
2. Kedua, seluruh informasi elektronik dan tanda tangan elektronik yang dihasilkan oleh suatu system informasi, termasuk print out-nya harus dapat menjadi alat bukti di pengadilan.
3. Ketiga, perlunya aspek perlindungan hukum terhadap Bank Sentral, dan lembaga perbankan/keuangan, penerbit kartu kredit/kartu pembayaran dan lembaga keuangan lainnya dari kemungkinan adanya gangguan dan ancaman kejahatanelektronik. Dalam UU ITE ini, perlindungan tersebut dapat dilakukan dengan mengkriminalisasi setiap penggunaan dan akses yang dilakukan secara illegal terhadap komputer institusi/lembaga tersebut, mengingat peranan yang sangat vital dari lembaga-lembaga keuangan dalam perekonomian dan dalam rangka menjaga tingkat kepercayaan masyarakat terhadap lembaga keuangan.
4. Keempat, perlunya ancaman pidana yang bersifat deterren terhadap tindak kejahatan elektronik (*Cybercrime*), sehingga dapat memberikan perlindungan terhadap integritas sistem dan nilai investasi yang telah dibangun dengan alokasi sumber daya yang cukup besar. [19]

Berdasakan penjelasan di atas analisi yang dapat penulis berikan yaitu Seiring perkembangan teknologi, kejahatan cyber mengalami evolusi dalam modus operandinya. Salah satu modus baru yang mengemuka adalah pembobolan rekening nasabah melalui internet banking dengan rekayasa informasi teknologi. Kejahatan ini memanfaatkan kelemahan sistem keamanan digital serta rendahnya literasi digital masyarakat untuk mencuri data dan dana korban. Penegakan hukum dalam menghadapi kejahatan ini memerlukan adaptasi teori dan praktik untuk memastikan efektivitasnya. Menurut Soerjono Soekanto, penegakan hukum adalah proses yang melibatkan tiga elemen utama: substansi hukum, struktur hukum, dan budaya hukum. Ketiganya saling berinteraksi dalam menentukan keberhasilan penegakan hukum yaitu:

1. Substansi hukum mencakup aturan yang ada, termasuk undang-undang dan regulasi terkait kejahatan cyber. Dalam konteks ini, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perbankan menjadi dasar hukum utama. Namun, keberhasilan penegakan hukum memerlukan pembaruan substansi agar relevan dengan modus kejahatan yang terus berkembang. Substansi hukum yang adaptif dapat memberikan dasar hukum yang lebih kuat dalam menghadapi modus kejahatan baru, seperti pengaturan khusus terhadap serangan phishing, penggunaan

[19] Urgensi Cyberlaw Di Indonesia Dalam Rangka Penanganan Cybercrime Di Sektor Perbankan, (Tim Perundang-undangan dan Pengkajian Hukum Direktorat Hukum Bank Indonesia, *Jurnal Buletin Hukum Perbankan Dan Kebanksentralan*, Vol. 4 No. 2, Tahun 2006, hlm. 23.

Formatted: Font: Italic
Formatted: Font: 12 pt
Formatted: List Paragraph, Indent: Left: 0 cm, Line spacing: single, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,63 cm + Indent at: 1,27 cm
Formatted: Font: 12 pt
Formatted: List Paragraph, Left, Indent: Left: 0 cm, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,63 cm + Indent at: 1,27 cm
Formatted: Font: 12 pt
Formatted: Font: 12 pt, Italic
Formatted: Font: 12 pt
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Justified, Indent: First line: 0,75 cm
Formatted: Font: Times New Roman, Italic
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, English (United States)

AI untuk kejahatan, atau pencurian data biometrik. Hal ini mencakup penyusunan peraturan pelaksana yang lebih rinci dan prosedur penyidikan yang lebih sesuai dengan kebutuhan penanganan kejahatan berbasis teknologi.

2. Struktur hukum mengacu pada aparat penegak hukum seperti polisi, jaksa, dan hakim. Penanganan kejahatan cyber menuntut peningkatan kapasitas teknis aparat dalam memahami teknologi informasi, termasuk teknik forensik digital untuk mengungkap kejahatan ini. Selain itu, koordinasi lintas lembaga seperti Otoritas Jasa Keuangan (OJK), Bank Indonesia, dan penyedia layanan teknologi informasi sangat penting untuk mendeteksi dan mencegah kejahatan sejak dini. Pelatihan berkelanjutan dan pembentukan unit khusus dalam kepolisian yang menangani kejahatan cyber dapat menjadi solusi untuk mengatasi tantangan teknis ini. Selain itu, perlu ada protokol standar untuk berbagi data antara lembaga pemerintah dan sektor swasta yang mendukung investigasi tanpa melanggar hak privasi.
3. Budaya hukum mencerminkan sikap masyarakat terhadap hukum. Dalam konteks kejahatan cyber, literasi digital masyarakat harus ditingkatkan agar lebih waspada terhadap ancaman rekayasa teknologi. Edukasi publik yang berkesinambungan melalui kampanye di media sosial, seminar, dan pelatihan komunitas dapat memberikan pemahaman lebih dalam mengenai bahaya berbagi informasi pribadi secara tidak hati-hati. Selain itu, sektor perbankan dan fintech juga harus berperan aktif dalam memberikan edukasi kepada nasabahnya terkait keamanan transaksi online.

CONCLUSION

1. Modus Kejahatan Cyber dalam Internet Banking Seiring dengan perkembangan teknologi informasi, modus kejahatan cyber terus mengalami transformasi. Salah satu bentuk kejahatan cyber yang meresahkan adalah rekayasa informasi teknologi, di mana pelaku kejahatan menggunakan metode teknis untuk membobol rekening nasabah melalui internet banking. Teknik yang digunakan bervariasi, mulai dari phishing, malware, hingga peretasan melalui kerentanan sistem. Tujuan utama para pelaku adalah mencuri informasi pribadi, seperti kata sandi dan kode otentikasi, untuk mendapatkan akses ke rekening nasabah dan mencuri dana.

~~1.~~2. Bank telah memberikan perlindungan kepada nasabah dari tindakan *phishing*, *pharming* dan *spoofing* melalui 2 (dua) cara, yaitu cara preventif dan represif. Perlindungan preventif yang diberikan oleh Bank berupa edukasi melalui platform media sosial resmi Bank. Kemudian dalam penerapan manajemen risikonya, Bank telah memenuhi cakupan sebagaimana diatur dalam Pasal 2 POJK Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum.

~~2.~~3. Dalam konteks kejahatan cyber, tantangan terbesar adalah penegakan hukum yang efektif, mengingat karakteristik kejahatan ini bersifat lintas batas, canggih, dan terus berkembang. Oleh karena itu, harus beradaptasi dengan tantangan era digital. Penegakan Hukum terhadap Kejahatan Cyber Penegakan hukum dalam menghadapi kejahatan cyber, khususnya yang menyasar rekening nasabah melalui internet banking, melibatkan beberapa tantangan dan faktor penting yang perlu diperhatikan Kerjasama Multinasional, Pembaruan Regulasi yang Dinamis, Teknologi Forensik Digital dan Bank dan lembaga keuangan memainkan peran penting dalam memastikan keamanan sistem internet banking.

Formatted: Font: 12 pt

Formatted: Font: Italic

REFERENCES

http://root.wanxp.netindex.phpoption, diakses pada tanggal 20 Februari 2024.
https://databoks.katadata.co.id/datapublish/2021/10/07/pengguna-bank-digital-di-indonesia-diproyeksi-capai-748-juta-pada-2026, di akses tanggal 6 Mei 2023
https://nasional.kompas.com/read/2022/09/16/02400071/kejahatan-siber--pengertian-karakteristik-dan-faktor-penyebabnya diakases tanggal 3 November 2023.
Hutagalung, Ami Yusfalina, Analisis Urgensi Cyberlaw Di Indonesia Dalam Rangka Penanganan Cybercrime Disektor Perbankan (Studi Pada PT. Bank Sumut KCP Syariah Jl. HM Joni), *Tesis,* Pascasarjana Universitas Halu Oleo, Tahun 2022.
Mudadi & Barda Nawawi, 2010, *Teori-teori dan Kebijakan Pidana*, PT. Alumni Bandung.
Muhammad Yakup, Abdul Gani, Emil Salim Siregar, Pengaturan Hukum Terhadap Layanan Internet Banking Dalam Transaksi Perbankan, *Jurnal Pionir LPPM Universitas Asahan Vol. 6 No. 1 Januari 2020, Program Studi Ilmu Hukum*, Fakultas Hukum, Universitas Asahan, Kisaran.
Rachmadi Usman, 2003, *Aspek-aspek Hukum Perbankan Indonesia*, Gramedia Pustaka, Jakarta.
Ronny Sautama Hotma Bako, 1995, *Hubungan Bank Dengan Nasabah Terhadap Produk Tabungan Dan Deposito*, Citra Aditya Bakti, Bandung.
T. Moore and R. Clayton, An empirical analysis of the current state of phishing attack and defence", *In Proceedings of the Sixth Workshop on the Economics of Information Security*, Vol. 4 No. 3, 2007.
Thor, Zero, *Knowledge Password*, 2008, PT Elex Media Komputindo Gramedia Kelompok Gramedia, Jakarta.
Umul Khair, Anny Yuserlina, Perlindungan Hukum Data Nasabah Internet Banking Di Bri Kota Bukittinggi Dan Payakumbuh, *Jurnal ensikopediaku Lembaga Penelitian dan Penerbitan Hasil Penelitian Ensiklopedia*, Vol. 1 No.2 Juni 2019 Sekolah Tinggi Ilmu Hukum Putri Maharaja Payakumbuh.
Vyctoria, 2013, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*, CV Andi Offset, Yogyakarta.

Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt, Italic
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt, Italic
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: 12 pt, Italic
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt, Italic
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt