KAJIAN YURIDIS TERHADAP KEJAHATAN PEMBOBOLAN REKENING DALAM KASUS PHISING DI SEKTOR PERBANKAN[1]

Oleh :
Yoanda Tesalonika Lendo[2]
Maarthen Youseph Tampanguma[3]
Dicky Janeman Paseki[4]

Abstrak

Perkembangan teknologi informasi yang pesat telah membawa kemudahan dalam sektor perbankan, khususnya dalam layanan digital. Namun, kemajuan ini juga diiringi dengan meningkatnya risiko kejahatan siber, salah satunya adalah kejahatan pembobolan rekening melalui modus *phishing*. Kajian ini bertujuan untuk menganalisis aspek yuridis terkait tindak pidana pembobolan rekening dengan modus *phishing* dalam sistem hukum Indonesia, serta meninjau efektivitas regulasi dan penegakan hukum yang berlaku. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan studi kasus. Hasil kajian menunjukkan bahwa modus *phishing* tergolong sebagai tindak pidana dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP), namun masih terdapat tantangan dalam pembuktian dan pelacakan pelaku karena sifat kejahatannya yang lintas batas dan anonim. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas aparat penegak hukum, serta sinergi antara otoritas perbankan, kepolisian, dan masyarakat dalam mencegah dan menanggulangi kejahatan ini. Kajian ini merekomendasikan perlunya pembaruan hukum dan peningkatan literasi digital sebagai langkah preventif terhadap kejahatan siber di sektor perbankan.

Kata kunci: phishing, pembobolan rekening, kejahatan siber, hukum perbankan

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah membawa dampak yang signifikan pada berbagai aspek kehidupan, termasuk di sektor perbankan. Dengan kemudahan akses dan penggunaan teknologi, masyarakat dapat melakukan transaksi perbankan dengan lebih mudah dan cepat. Namun, perkembangan teknologi ini juga membawa risiko keamanan yang lebih tinggi, terutama dalam hal kejahatan pembobolan rekening dalam kasus phising. Para penjahat dunia maya ini memiliki lingkungan potensi yang tinggi di bagiannya sehingga sulit untuk menelusuri dan memusnahkannya secara bersih, Serangan tersebut menimbulkan unsur kejahatan yang berakibat munculnya tindak pidana baru terhadap bidang teknologi informasi dan komunikasi.

Tindak pidana ITE merupakan suatu tindak pidana yang dalam pelaksanaannya terdapat unsur komputer atau alat elektronik lainnya yang terkoneksi melalui perangkat telekomunikasi dalam bentuk internet online yang menjadi media bagi seseorang atau kelompok untuk melakukan pelanggaran dan/atau kejahatan.[5]

Lahirnya Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Eleketronik sebagaimana telah diubah oleh Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik didasarkan amanat yang terkandung pada Pasal 28F Undang-undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan “Setiap orang berhak untuk berkomunikasi dan memperoleh informasi dengan baik untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk

---

[1] Artikel Skripsi
[2] Mahasiswi Fakultas Hukum Unsrat, NIM 21071101010623
[3] Fakultas Hukum Unsrat, Dosen Ilmu Hukum
[4] Fakultas Hukum Unsrat, Dosen Ilmu Hukum

[5] Maskun, *Kejahatan Siber (cyber crime)*, Prenada Media, Jakarta, 2013, hlm. 50

mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.

Perkembangan teknologi informasi dan komunikasi (TIK) di dunia sangat bermanfaat bagi berbagai sektor industri, perbankan dan usaha kecil dan menengah (UKM). Sektor-sektor ini mendapat manfaat dari efisiensi dan efektivitas dalam hal operasi serta peningkatan pengalaman pengguna. Namun perkembangan ini menimbulkan masalah baru dengan munculnya berbagai cybercrime oleh pihak-pihak yang mencoba memanfaatkan kelemahan sistem dan kesadaran pengguna tentang sistem informasi.

Salah satu bentuk kejahatan dunia maya yang dilakukan oleh scammers adalah phishing. Phishing adalah aktivitas kriminal yang menggunakan teknik rekayasa sosial.[6] Insiden phishing marak terjadi pada layanan perbankan online di bank-bank di Indonesia. Kepala Otoritas Jasa Keuangan melaporkan, sejak tahun 2013, pengguna merugi Rp 100 miliar akibat kasus pencurian dengan "phishing" (PT. Kompas Cyber Media, 2015).

Manusia yang berada hampir di seluruh belahan dunia sangat bergantung dengan keberadaan internet bahkan dengan menggunakan jaringan internet, telah mampu membentuk budaya baru di dalam kehidupan. Internet merubah pekerjaan sehari-hari menjadi lebih mudah dalam berbagai sektor mulai dari kegiatan perdagangan, bisnis, pembayaran atau transaksi perbankan yang dapat dimanfaatkan untuk kepentingan pribadi, instansi/perusahaan atau pun pemerintahan. Semakin banyaknya aktifitas yang dimanfaatkan oleh internet ini, mengakibatkan peningkatan pengguna internet di seluruh dunia. Oleh karena itu, berkenaan dengan pembangunan, kemajuan dan perkembangan teknologi informasi melalui internet, peradaban manusia diperhadapkan pada fenomena-fenomena baru yang mampu mengubah hampir setiap aspek kehidupan manusia.6.Istilah kejahatan yang terjadi dalam sebuah transaksi elektronik ini biasa dikenal dengan cyber crime. Bentuk kejahatan ini mengkhawatirkan sampai ke berbagai negara di dunia karena segala perkara yang terjadi berbeda ruang maupun waktu sehingga kebanyakan korban maupun penegak hukum harus mempunyai kemampuan ekstra untuk menyikapi kejahatan ini. Phising merupakan salah satu bentuk kejahatan yang juga harus diwaspadai karena ketelitian dalam penggunaan media elektronik merupakan faktor utama agar tidak terjerat phising ini.[7]

Informasi dan Transaksi Elektronik merupakan salah satu yang sering digunakan dalam kehidupan sehari-hari bisa berupa handphone, laptop, internet, internet banking, media sosial (yang mencakup dalam jaringan internet), e-money, dan lain-lain yang mencakup tentang elektronik dan informasi. Dalam hal ini selalu ada batasan dan peraturan dalam penggunaan informasi dan transaksi elektronik. Pembuatan peraturan perundang-undangan terhadap pemanfaatan Teknologi Informasi dan Transaksi Elektronik memerlukan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Dan untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan keamanan dan ketertiban umum dalam suatu masyarakat. Pembuatan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan

[6] Amin Muftiadi, Tri Putri Mulyani Agustina, Margaretha Evi, analisis ancaman phising terhadap layanan online banking" Jurnal Ilmiah Teknik (agustus 2022),hal.1

[7] Malunsenge, Leticia, Cornelis Massie, and Ronald Rorie. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia." *Lex Crimen* 11.3 (2022).

Transaksi Elektronik agar terwujud keadilan, ketertiban umum, dan kepastian hukum. Dalam membuat undang-undang dan mengatur pasal demi pasal tersebut untuk mengantisipasi dan mengatur sistem hukum terhadap kejahatan yang sering terjadi dalam dunia maya yang biasa di sebut dengan "kejahatan di dunia maya" atau sering disebut Cyber Crime, harus adanya ketegasan dalam pemberantasan kejahatan terhadap Cyber dan menindak suatu pebuatan Cyber Crime yang dilakukan oleh pelaku, hal ini untuk membangun kepercayaan masyarakat terhadap penggunaan komputer dan jaringan komputer agar tidak ada halangan saat memakai hal tersebut.

Sampai saat ini, Indonesia belum memiliki undang – undang khusus yang mengatur tentang cyber crime. Namun demikian, terdapat beberapa hukum positif yang berlaku umum dan dapat dikenakan kepada pelaku cyber crime yang menggunakan sarana internet. Karena tindak pidana cyber crime melibatkan beberapa perbuatan sekaligus, maka Pasal–Pasal dalam KUHP dapat digunakan beberapa pasal sekaligus yaitu, pasal 362 KUHP tentang pencurian, pasal 378 KUHP tentang Perbuatan Curang, Pasal 369 KUHP tentang Pemerasan dan Pengancaman, Pasal 372 KUHP tentang Penggelapan (Akub, M. S., 2020).[8] Salah satu yang sering terjadi antara lain adalah Cyber Crime Phising, masyarakat sering tidak menyadari kejahatan Cyber Crime Phising sangat merugikan bagi korban yang pernah mengalami kejahatan ini. Phising (password harvesting fishing) adalah tindak kejahatan penipuan dengan memanfaatkan email palsu atau situs website palsu yang bertujuan untuk mengelabui user lain. Pemanfaatan email palsu atau website palsu ini ditujukan untuk mendapatkan data user tersebut. Penggunaan data user seringkali untuk mengirim email yang seolah-olah berasal dari sebuah perusahaan resmi, misalnya bank dengan tujuan untuk mendapatkan data-data pribadi seseorang, misalnya User ID, PIN, nomor rekening, nomor kartu kredit dan sebagainya.

Cyber Crime Phising biasanya dilakukan dengan menyamar sebagai orang lain, biasanya dengan situs web palsu atau link palsu untuk menipu seseorang untuk mendapatkan atau mencuri informasi pribadi. Pada hal ini, penyerang mengirimkan email yang seolah-olah berasal dari nama logo perusahaan atau layanan web yang biasa digunakan oleh seseorang. Baris subjek bisa berupa "silahkan masukan user ID / password anda", dalam tautan yang berbeda, Email tersebut biasanya merupakan tautan phising yang seolah-olah ditujukan ke situs web anda, tetapi sebenarnya ditujukan ke situs penipuan.

Dalam Undang-Undang No. 19 Tahun 2016 tentang perubahan atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dirumuskan bahwa:

Pasal 30 UU ITE Setiap orang yang dengan sengaja dan tanpa hak melakukan perbuatan yang mengakibatkan kerugian atau kehilangan bagi orang lain dengan cara:

1. Mengakses Komputer dan/atau Sistem Elektronik milik orang lain tanpa hak.
2. Mengakses Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain tanpa hak.
3. Mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara melanggar, menerobos, melampaui, atau menjebol Sistem Pengamanan.Dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pasal 28 UU ITE Setiap orang yang dengan sengaja dan tanpa hak melakukan perbuatan penipuan elektronik dengan cara:

1. Mengirimkan Informasi Elektronik yang tidak benar atau menyesatkan.
2. Menggunakan Identitas Elektronik

[8] Angela Gabriela Bupu," Analisis Yuridis Cyber Crime Pembobolan Dana Nasabah pada Aplikasi Mobile Banking dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu",Jurnal Ilmu Hukum dan Sosial Vol.2, No.2(Mei,2024),hal.2

orang lain.

3. Menggunakan Informasi Elektronik yang tidak benar atau menyesatkan untuk memperoleh keuntungan.Dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pasal 30 Ayat 1 UU ITE : "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun". yang dilakukan dengan cara:

- Menggunakan teknologi informasi dan transaksi elektronik untuk melakukan penipuan.
- Menggunakan identitas palsu atau identitas orang lain untuk melakukan penipuan.
- Menggunakan teknik phising, spoofing, atau teknik lainnya untuk melakukan penipuan.
- Menggunakan aplikasi atau perangkat lunak palsu untuk melakukan penipuan.
- Menggunakan jaringan komputer atau sistem elektronik untuk melakukan penipuan.

Adapun perkara atau kasus yang pernah terjadi dalam Cyber Crime Phising, yaitu pencurian UserID seseorang dengan berkedok penipuan link untuk melakukan kejahatan yang berupa modus operandi. Pelaku phising tersebut menggunakan modus ini dengan mengirimkan email dan sms yang mengaku dari pihak bank dan meminta korban untuk mengupdate data pribadi dan mengirimkan OTP, korban percaya pada email dan sms tersebut,korban mengklik link atau mengunduh file yang terkait dengan email dan sms tersebut, yang kemudian mengarahkan mereka ke situs web palsu yang terlihat seperti situs web bank,lalu korban menginput informasi pribadi seperti username,password, dan kode OTP ke situs web palsu tersebut ,setelah menginput informasi pribadi korban mengalami kerugian seperti uang yang hilang di rekening bank atau informasi pribadi yang dicuri, lalu korban melaporkan ke pihak bank dan meminta bantuan setelah itu melaporkan juga ke pihak kepolisian untuk menangkap pelaku dan polisi berhasil menangkap pelaku phising tersebut dan mengamankan barang bukti berupa laptop,handphone, dan dokumen palsu.

Dalam hal ini pula menyatakan terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana cyber crime, sebagaimana diatur dan diancam pidana dalam Pasal 27 dan Pasal 28 ayat Undang-undang Republik Indonesia No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik .

Dilihat dari contoh kasus atau perkara diatas, putusan Majelis Hakim Pengadilan Negeri Medan dengan Putusan No: 3006/Pid.Sus/2017/PN.Mdn, memutuskan untuk menjatuhi hukuman terhadap pelaku dengan tindak pidana Cyber, yang berawal dari Phising dengan tujuan untuk mengambil data korban dan membobol rekening korban, mencuri uang korban. Sanksi pidana yang diberikan oleh Majelis Hakim Pengadilan Negeri Medan menjatuhkan hukuman pidana penjara empat (4) tahun dan denda sebesar Rp 500.000.000,- (lima ratus juta rupiah), Terdakwa dihukum membayar uang penganti sebesar Rp 100.000.000,- (seratus juta rupiah) kepada korban.

Situasi ini menunjukkan bahwa bank mengambil posisi bahwa kejadian tersebut bukanlah hasil dari kesalahan dalam layanan perbankan yang mereka sediakan, sehingga tanggung jawab atas kerugian tersebut tidak dapat ditangani oleh bank (Ali, 2023).[9]

B. Rumusan Masalah

1. Bagaimana Pengaturan Hukum dalam Penanggulangan kejahatan

[9] Ramadhanti Achlina Tri Putri, Heru Sugiyon, TANGGUNG JAWAB BANK TERHADAP TINDAKAN PHISINGDALAM SISTEM PENGGUNAAN E-BANKING(STUDI: KASUS PHISINGPADA PT. BANK RAKYAT INDONESIA (PERSERO) TBK).

pembobolan rekening dalam kasus phising di sektor perbankan?
2. Bagaimana Penegakan Hukum pada Kejahatan Pembobolan Rekening dalam Kasus Phising di sektor Perbankan ?

C. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah menggunakan metode penelitian hukum normatif yaitu yang dimana pengkajiannya berdasarkan atas bahan-bahan hukum dari literatur.

PEMBAHASAN

A. Pengaturan Hukum Dalam Penanggulangan Kejahatan Pembobolan Rekening dalam Kasus Phising Di Sektor Perbankan

Perkembangan teknologi informasi dan komunikasi telah membawa dampak yang signifikan pada berbagai aspek kehidupan, termasuk di sektor perbankan. Dengan kemudahan akses dan penggunaan teknologi, masyarakat dapat melakukan transaksi perbankan dengan lebih mudah dan cepat. Namun, perkembangan teknologi ini juga membawa risiko keamanan yang lebih tinggi, terutama dalam hal kejahatan pembobolan rekening dalam kasus phising.[10]

Dalam era perkembangan teknologi yang semakin pesat, digitalisasi telah menjadi bagian tak terpisahkan dari berbagai sektor, termasuk perbankan. Sistem perbankan digital, yang mengandalkan teknologi informasi untuk memberikan layanan perbankan secara online, dirancang untuk mempermudah transaksi finansial, mulai dari transfer uang hingga pengelolaan investasi. Namun, di balik kemudahan ini, ancaman kejahatan siber seperti phishing semakin marak terjadi.
Berikut merupakan ciri-ciri phising:

1. Menyamar sebagai institusi resmi
2. Mencantumkan nominal uang yang sangat besar
3. Memenangkan undian fantastis
4. Memanfaatkan emosi korban
5. Kalimat ajakan terkesan memaksa
6. Menyamar sebagai orang yang dikenal
7. Tidak mencantumkan nama penerima

Menurut Bapak A.R Hakim Rambe bahwa upaya penanggulangan dapat ditempuh dengan 1) Penerapan hukum pidana; 2) Pencegahan tanpa pidana; dan 3) Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui media masa. Untuk kategori pertama dikelompokkan ke dalam upaya penanggulangan kejahatan lewat jalur penal, sedangkan kedua dan ketiga termasuk upaya penanggulangan kejahatan melalui jalur non penal. Upaya melalui jalur penal merupakan upaya represif yang dalam pelaksanaannya mengandung keterbatasan sehingga perlu diimbangi dengan pendekatan non-penal yang cenderung merupakan upaya preventif. Kejahatan telah diterima sebagai suatu fakta yang merugikan bagi masyarakat yaitu korban. Kerugian yang ditimbulkan itu dapat berupa kerugian dalam arti materiil maupun moril. Kerugian materiil berupa timbulnya korban kejahatan dan rusak atau musnahnya berat benda serta meningkatnya biaya yang harus dikeluarkan bagi penanggulangannya. Kerugian moral berupa berkurang atau hilangnya kepercayaan masyarakat terhadap pelaksanaan penegakan hukum yang dilakukan oleh aparat hukum.[11]

Kewajiban Bank Selanjutnya terkait kewajiban bank sebagai pelaku usaha, selain mengelola dana nasabah dengan baik, juga ditentukan dalam Pasal 7 Undang-Undang Perlindungan Konsumen, sebagai berikut:

a) Beritikad baik dalam melakukan kegiatan usahanya,
b) Memberikan kondisi dan jaminan barang dan atau jasa serta

[10] Maskun, *Kejahatan Siber (cyber crime)*, Prenada Media, Jakarta, 2013, hlm. 50

[11] Purwanti, Y., Rachman, F., Gunawan, T., & Kartadinata, A. (2023). Upaya Penanggulangan Tindak Pidana Penipuan Dengan Metode Phising Oleh Kepolisian Daerah Lampung. *Audi Et AP: Jurnal Penelitian Hukum*, *2*(01), 64-71.

memberi penjelasan penggunaan, perbaikan dan pemeliharaan,
c) Memperlakukan atau melayani konsumen secara benar dan jujur serta tidak diskriminatif
d) Menjamin mutu barang dan atau jasa yang diproduksi dan atau diperdagangkan ketentuan standar mutu barang dan atau jasa yang berlaku,
e) Memberi kesempatan kepada konsumen untuk menguji dan atau mencoba barang dan atau jasa tertentu serta memberi jaminan dan atau garansi atas barang yang dibuat dan atau jasa yang diperdagangkan
f) Memberi kompensasi, ganti rugi dan atau penggantian atas kerugian akibat penggunaan, pemakaian dan pemanfaatan barang dan atau jasa yang diperdagangkan,
g) Memberi kompensasi, ganti rugi dan atau penggantian apabila barang dan atau jasa yang diterima atau dimanfaatkan tidak sesuai dengan perjanjian.

Penanggulangan kejahatan phising pembobolan rekening dapat dilakukan melalui beberapa cara:

Upaya Pencegahan
a) Edukasi masyarakat: Meningkatkan kesadaran masyarakat tentang bahaya phising dan cara-cara untuk menghindarinya.
b) Pengamanan sistem: Meningkatkan keamanan sistem perbankan dan keuangan dengan menggunakan teknologi keamanan yang canggih.
c) Autentikasi dua faktor: Menggunakan autentikasi dua faktor untuk meningkatkan keamanan akses ke rekening.

Upaya Penindakan
a) Kerja sama dengan aparat penegak hukum: Melaporkan kasus phising kepada aparat penegak hukum dan bekerja sama dalam proses penyidikan.
b) Pengembangan regulasi: Mengembangkan regulasi yang lebih efektif untuk mengatur dan mengawasi kegiatan keuangan online.
c) Sanksi yang tegas: Memberikan sanksi yang tegas bagi pelaku kejahatan phising.

Upaya Pemulihan
a) Pemulihan rekening: Memulihkan rekening yang telah dibobol dan mengembalikan dana yang hilang.
b) Pengawasan rekening: Meningkatkan pengawasan rekening untuk mencegah kejahatan phising yang sama terjadi lagi.
c) Pemberian informasi: Memberikan informasi kepada nasabah tentang kejahatan phising dan cara-cara untuk menghindarinya.

Phishing adalah upaya penipuan yang dilakukan dengan cara mengelabui korban agar memberikan informasi pribadi atau data sensitif, seperti nomor kartu kredit, kata sandi, atau identitas pribadi lainnya. Tindakan ini sering kali dilakukan melalui email, situs palsu, atau pesan yang tampak meyakinkan. Fenomena phishing di sektor perbankan digital erat kaitannya dengan meningkatnya ketergantungan pada teknologi dan data elektronik. Ketika sistem digital menjadi tulang punggung transaksi keuangan, risiko kebocoran data pribadi pun meningkat. Pelaku phishing memanfaatkan celah keamanan atau kurangnya kesadaran pengguna untuk mencuri informasi yang kemudian disalahgunakan untuk keuntungan pribadi. Dalam konteks perbankan digital data yang dicuri dapat berupa kredensial akun, informasi rekening, hingga data keuangan lainnya yang bersifat sangat sensitif. Phising bisa terjadi akibat dari perilaku transaksi ekonomi yang didasari dengan niat yang tidak baik serta lembaga perbankan yang belum bisa menjamin dan menjaga kerahasiaan pemilik dan terkait kepemilikan dana yang tersimpan di bank tersebut. Selanjutnya Bapak A.R Hakim Rambe

juga menyatakan bahwa penyidikan tindak pidana penipuan melalui metode phising berlaku penyidikan tindak pidana cybercrime pada umumnya Penyidikan terhadap tindak pidana cybercrime pada umunya juga selain dilaksanakan berdasarkan ketentuan yang diatur mengenai penyidikan yang tedapat dalam Kitab Undang Undang Hukum Acara Pidana juga dilaksanakan berdasarkan ketentuan khusus mengenai penyidikan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, hal ini dilakukan agar penyidikan dan hasilnya dapat diterima secara hukum. Berikut adalah beberapa hal mengenai penyidikan yang diatur dalam Undang – Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik : 1. 2. 3. Pasal 43 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa yang diizinkan untuk melakukan penyidikan di dalam undang -undang ini adalah penyidik Kepolisian Negara Republik Indonesia dan pejabat pegawai negeri sipil tertentu yang lingkup tugas dan tanggung jawabnya di bidang teknologi dan transaksi elektronik. Pasal 43 Ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa penyidikan terhadap tindak pidana cyber crime harus memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan undangan. perundang Pasal 43 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa 68 Upaya Penanggulangan Tindak Pidana Penipuan Dengan Metode Phising Oleh Kepolisian Daerah Lampung penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan setempat. Pasal 43 Ayat (6) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa dalam hal melakukan penangkapan penahanan, penyidik dan melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.[12]

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

[12] Purwanti, Y., Rachman, F., Gunawan, T., & Kartadinata, A. (2023). Upaya Penanggulangan Tindak Pidana Penipuan Dengan Metode Phising Oleh Kepolisian Daerah Lampung. *Audi Et AP: Jurnal Penelitian Hukum*, *2*(01), 64-71.

B. Penegakan Hukum Pada Kejahatan Pembobolan Rekening Dalam Kasus Phising Di Sektor Perbankan

Kemajuan teknlogi informasi saat ini memberikan kemudahan bagi masyarakat untuk mengaskes informasi darimanapun. Perkembangan teknologi informasi juga menuntut masyarakat untuk dapat mengikuti perkembangannya. Disamping banyaknya manfaat yang ditimbulkan dari perkembangan tersebut juga lahirlah dampak negatif dalam penyalahgunaan teknologi. Dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.[13]

Terdapat 3 unsur dalam penegakan hukum menurut Sudikno Mertokusumo, yaitu kepastian hukum, kemanfaatan, dan keadilan. Penegakan hukum dalam kejahatan pembobolan rekening kasus phishing di Indonesia didasarkan pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-Undang Hukum Pidana (KUHP), dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pelaku phishing dapat dijerat dengan berbagai pasal pidana, termasuk penipuan, manipulasi, dan penerobosan sistem.

Perbuatan tindak pidana cybercrime di Indonesia ditandai dengan pembentukan undang undang khusus yaitu Undang-Undang Nomor 19 Tahun 2016 tentang ITE. berdasarkan asas "Lex Specialis Derogat Legi General" yang berarti bahwa undang-undang yang bersifat khusus dapat mengesampingkan undang-undang yang bersifat umum. Sehingga yang berlaku saat ini adalah UU ITE dalam menangani kasus tindak pidana cyber crime. UU ITE yang dikenakan kepada pelaku phising jenisnya adalah tindak pidana penjara dan tindak pidana denda, tidak adanya ancaman sanksi pidana tambahan. Jadi sistem pidana yang dipakai tidak ada inovasi jenis sanksi pidana yang khas untuk tindak pidana di bidang informasi dan transaksi elektronik.[14]

Sebelum UU ITE dibuat, penegakan hukum terhadap pelaku cyber crime menggunakan ketentuan dalam KUHP dengan menerapkan pasal yang memiliki kesesuaian unsur. Dalam KUHP ketentuan pidana cyber crime yang berbentuk phising dapat menggunakan ketentuan pasal 378 tentang penipuan. Hal ini karena phising secara umum juga merupakan bentuk tindakan penipuan. Pasal 378 dirumukan "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun".

Penegakan hukum yaitu suatu keadaan dalam menyerasikan kaidah-kaidah hukum dari nilai-nilai luhur terhadap tindakan yang lahir ditengah-tengah kehidupan bermasyarakat sehingga, dengan keberadaan negara Indonesia sebagai negara hukum dapat membuktikan tujuan akhir dari hukum itu sendiri yaitu suatu bentuk penciptaan ketertiban dan kedamaian hidup dalam bermasyarakat melalui penegakan hukum dan perlindungan hukum.Cyber crime atau dengan istilah lain yaitu kejahatan dunia maya dalam peraturan untuk transaksi elektronik yakni UU ITE, tidak mengatur secara jelas bentuk perlindungan bagi para korban atas kejahatan dalam sebuah transaksi elektronik tersebut. Untuk cyber crime berbentuk phising adalah jenis kejahatan yang dapat mengakibatkan kerugian terhadap korban-korbannya secara materiil, seperti data pribadi. Pada dasarnya, data pribadi dilindungi berdasarkan peraturan

[13] Siswanto Sunarso, Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari, PT. Rineka Cipta, Jakarta, 2009

[14] Supanto, Perkembangan Kejahatan Teknologi Informasi(Cyber Crime) dan Antisipassinya dengan Penal Policy, Yustisia Jurnal Hukum , No 1, 2016

perundang-undangan di Indonesia. Oleh karena itu, ketika kerahasiaan terhadap suatu (barang) hak milik tidak lagi sempurna maka membutuhkan perlindungan hukum dalam bentuk perlindungan kepada pihak-pihak yang dirugikan.

Hukum tidak dapat dikenakan apabila hukumnya mengalami kekaburan seperti Pasalnya memiliki penafsiran yang bermacam-macam dan/atau konsepnya belum ada. Bagaimana dapat diterapkan suatu aturan terhadap pelaku tindak pidana jika hukumnya tidak tegas dan jelas. Berdasarkan uraian yang telah dijelaskan di atas, maka Kebijakan Hukum yang dilakukan terhadap Konsep Phising dan Pasal 35 berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah:

1. Konsep Phising Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan dan perubahan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik. Menggunakan media yang terhubung ke jaringan internet yang berisikan Nama Domain dari Informasi Elektronik dan/atau Dokumen Elektronik yang menggerakkan orang lain untuk mengakses Informasi Elektronik dan/atau Dokumen Elektronik tersebut untuk memasukkan identitas pribadi rahasia ke dalam Informasi Elektronik dan/atau Dokumen Elektronik, sehingga menyebabkan orang tersebut mengalami kerugian.
2. Pasal 35 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan Phising mengakibatkan kerugian bagi orang lain. Berdasarkan Kebijakan Hukum diatas maka dapat diketahui apa yang dimaksud dengan phising dan bagaimana pengaturannya terhadap cyber crime dalam bentuk phising. Lalu, kita dapat menentukan syarat dapat dikriminalisasikan pelaku phising yaitu apabila telah melanggar ketentuan hukum Pasal 35 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah dilakukannya kebijakan hukum terhadap Pasal 35 dan kemudian tidak terjadi kembali kekaburan norma didalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Cyber crime dalam bentuk Phising ini juga tidak dirumuskan didalam Rancangan Kitab UndangUndang Hukum Pidana, mungkin dikarenakan terkait teknologi informasi sehingga tidak diaturnya mengenai phising.

Adapun perkara atau kasus yang pernah terjadi dalam Cyber Crime Phising, yaitu pencurian UserID seseorang dengan berkedok penipuan link untuk melakukan kejahatan yang berupa modus operandi. Pelaku phising tersebut menggunakan modus ini dengan mengirimkan email dan sms yang mengaku dari pihak bank dan meminta korban untuk mengupdate data pribadi dan mengirimkan OTP, korban percaya pada email dan sms tersebut,korban mengklik link atau mengunduh file yang terkait dengan email dan sms tersebut, yang kemudian mengarahkan mereka ke situs web palsu yang terlihat seperti situs web bank,lalu korban menginput informasi pribadi seperti username,password, dan kode OTP ke situs web palsu tersebut ,setelah menginput informasi pribadi korban mengalami kerugian seperti uang yang hilang di rekening bank atau informasi pribadi yang dicuri, lalu korban melaporkan ke pihak bank dan meminta bantuan setelah itu melaporkan juga ke pihak kepolisian untuk menangkap

pelaku dan polisi berhasil menangkap pelaku phising tersebut dan mengamankan barang bukti berupa laptop,handphone, dan dokumen palsu.

Dalam hal ini pula menyatakan terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana cyber crime, sebagaimana diatur dan diancam pidana dalam Pasal 27 dan Pasal 28 ayat Undang-undang Republik Indonesia No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik .

Dilihat dari contoh kasus atau perkara diatas, putusan Majelis Hakim Pengadilan Negeri Medan dengan Putusan No: 3006/Pid.Sus/2017/PN.Mdn, memutuskan untuk menjatuhi hukuman terhadap pelaku dengan tindak pidana Cyber, yang berawal dari Phising dengan tujuan untuk mengambil data korban dan membobol rekening korban, mencuri uang korban. Sanksi pidana yang diberikan oleh Majelis Hakim Pengadilan Negeri Medan menjatuhkan hukuman pidana penjara empat (4) tahun dan denda sebesar Rp 500.000.000,- (lima ratus juta rupiah), Terdakwa dihukum membayar uang penganti sebesar Rp 100.000.000,- (seratus juta rupiah) kepada korban.[15]

PENUTUP

A. Kesimpulan

Berdasarkan pembahasan yang telah penulis jabarkan pada bab sebelumnya, maka dapat diambil kesimpulan sebagai berikut :

1. Pengaturan hukum tentang kejahatan phising di Indonesia telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 yang kemudian diubah menjadi Undang-Undang Nomor 9 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan lainnya. Pengaturan hukum ini bertujuan untuk melindungi masyarakat dari kejahatan phising dan memberikan sanksi bagi pelaku kejahatan. penanggulangan tindak pidana penipuan melalui metode phising dapat menggunakan kebijakan penal atau pun non penal. masyarakat harus berhati-hati dengan email, menggunakan password yang kuat, menggunakan autentikasi dua faktor, mengupdate software, menggunakan antivirus.
2. Penegakan hukum pidana terhadap serangan phising pada layanan online banking ini berupa : Ancaman pidana bagi pelaku (phisher) yang diatur sesuai dengan UU yang berlaku. Dan penyelesaian perkara kasus seperti ini melibatkan beberapa tahapan, dimulai dari pelaporan, penyidikan, penuntutan, persidangan sampai putusan. Efektivitas Penegakan Hukum terhadap Tindak Pidana Perbankan Dalam beberapa kasus, bank justru menolak untuk mengganti dana nasabah yang hilang dengan alasan kelalaian pribadi, seperti penyalahgunaan PIN atau OTP.

B. SARAN

Adapun saran yaitu antara lain sebagai berikut :

1. Dalam bidang hukum diperlukan suatu pembaharuan regulasi yang dapat mengakomodi jalanya kehidupan masyarakat . Dan penanggulangannya seperti: Peningkatan kesadaran masyarakat tentang bahaya phising dan cara-cara untuk menghindarinya, harus meningkatkan keamanan sistem perbankan dan keuangan dengan menggunakan teknologi keamanan yang canggih. Meningkatkan kerja sama antara lembaga penegak hukum, perbankan, dan keuangan untuk menangani kasus-kasus phising. Perbankan sebagai lembaga vital yang memiliki tugas menghimpun dan menyalurkan dana

[15] Ramadhanti Achlina Tri Putri, Heru Sugiyon, TANGGUNG JAWAB BANK TERHADAP TINDAKAN PHISING DALAM SISTEM PENGGUNAAN E-BANKING(STUDI: KASUS PHISINGPADA PT. BANK RAKYAT INDONESIA (PERSERO) TBK).

masyarakat sudah seharusnya meningkatkan kembali sistem keamanan agar tidak mudah terserang kejahatan siber yang semakin berkembang pesat modus operandinya.

2. Penegakan hukum atau perlindungan hukum yang diberikan kepada korban, berupa sanksi atau hukuman untuk pelaku tindak pidana pencurian data (phising) berdasarkan pasal 378 KUHP, Pasal 28 UU ITE, dan Pasal 35 UU ITE. Diperlukan peraturan yang lebih jelas serta perlindungan hukum yang lebih tegas. Pemerintah perlu melakukan perbaikan dalam Undang-Undang ITE agar mempertegas pengaturan tindak pidana cyber berupa phising agar kejahatan tersebut tidak terus terjadi dan merugikan banyak masyarakat. Perlunya memberikan kepastian hukum agar tidak terjadi kekaburan hukum. juga perlu meningkatkan pengetahuan masyarakat terkait kasus seperti ini, Masyarakat dalam hal ini juga perlu meningkatkan kewaspadaan terkait kejahatan phising.

DAFTAR PUSTAKA

Buku

Maskun. (2013). *Kejahatan siber (cyber crime)*. Jakarta: Prenada Media.

Sunarso, S. (2009). *Hukum informasi dan transaksi elektronik: Studi kasus Prita Mulyasari*. Jakarta: PT Rineka Cipta.

Jurnal

Achlina, R. T. P., & Sugiyon, H. (2023). Tanggung jawab bank terhadap tindakan phishing dalam sistem penggunaan e-banking (Studi: Kasus phishing pada PT. Bank Rakyat Indonesia (Persero) Tbk).

Angela Gabriela Bupu," Analisis Yuridis Cyber Crime Pembobolan Dana Nasabah pada Aplikasi Mobile Banking dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu",Jurnal Ilmu Hukum dan Sosial Vol.2, No.2(Mei,2024),

Amin Muftiadi, Tri Putri Mulyani Agustina, Margaretha Evi, analisis ancaman phising terhadap layanan online banking" Jurnal Ilmiah Teknik (agustus 2022),

Bupu, A. G. (2024). Analisis yuridis cyber crime pembobolan dana nasabah pada aplikasi mobile banking dengan modus pembobolan jalur undangan pernikahan palsu. *Jurnal Ilmu Hukum dan Sosial*, 2(2), 2.

Malunsenge, L., Massie, C., & Rorie, R. (2022). Penegakan hukum terhadap pelaku dan korban tindak pidana cyber crime berbentuk phishing di Indonesia. *Lex Crimen*, 11(3).

Muftiadi, A., Agustina, T. P. M., & Evi, M. (2022, Agustus). Analisis ancaman phishing terhadap layanan online banking. *Jurnal Ilmiah Teknik*, 1.

Purwanti, Y., Rachman, F., Gunawan, T., & Kartadinata, A. (2023). Upaya penanggulangan tindak pidana penipuan dengan metode phishing oleh Kepolisian Daerah Lampung. *Audi Et AP: Jurnal Penelitian Hukum*, 2(01), 64–71.

Supanto. (2016). Perkembangan kejahatan teknologi informasi (cyber crime) dan antisipasinya dengan penal policy. *Yustisia Jurnal Hukum*, (1).