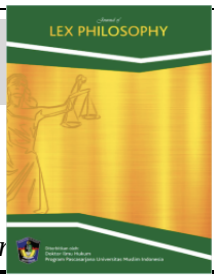
Journal of Philosophy (JLP)
Volume 4, Nomor 1, Juni 2023
P-ISSN: 2722-1237, E-ISSN: 2722-2020
Website: http: pasca-umi.ac.id/index.php/jlp
This work is licensed under a Creative Commons Attribution 4.0 International Licen



Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi *(Phising)* Di Lingkungan Perbankan

Lilis Ekayani[1], Hardianto Djanggih[2] & Moh. Akli Suong[3]

[1]*Magister Ilmu Hukum, Universitas Muslim Indonesia, Indonesia*
[1]*Fakultas Hukum, Universitas Muslim Indonesia, Indonesia*
[3]*Fakultas Hukum, Universitas Muslim Indonesia, Indonesia*
[*]*Koresponden Penulis, E-mail: lilis.ekayani@gmail.com*

ABSTRAK

Tujuan Penelitian menganalisis efektivitas Perlindungan Hukum Nasabah Terhadap Kejahatan Phising Di Lingkungan Perbankan Wilayah Bank Rakyat Indonesia Kantor Cabang Watansoppeng. Penelitian ini menggunakan metode hukum empiris. Hasil penelitian ini menunjukkan bahwa: (1) perlindungan hukum nasabah terhadap kejahatan phising di lingkungan perbankan kantor cabang watansoppeng hanya mendapatkan perlindungan preventif dan perlindungan represif belum efektif (2) faktor yang mempengaruhi efektifitas perlindungan hukum nasabah terhadap kejahatan phising adalah sistem keamanan yang masih perlu ditingkatkan, masih rendahnya pengetahuan tentang kejahatan tersebut,dan rendahnya kesadaran budaya privasi berjejaring sosial. Rekomendasi penelitian Kemampuan penegak hukum maupun sistem yang digunakan dalam menangani kejahatan siber harus mempuni untuk dapat mengimbangi perkembangan teknologi yang semakin maju.

Kata Kunci: *Nasabah; Data Pribadi; Perbankan*

ABSTRACT

The Research objective to analyze the effectiveness of legal protection for customers against phishing crimes in the regional banking environment of Bank Rakyat Indonesia, Watansoppeng branch office. This research uses empirical law method. The results of this study indicate that: (1) legal protection for customers against phishing crimes in the banking environment at the Watansoppeng branch office only gets preventive protection and repressive protection is not yet effective (2) factors that influence the effectiveness of legal protection for customers against phishing crimes are security systems that still need to be improved , low knowledge about the crime, and low awareness of social networking privacy culture. Research recommendations The ability of law enforcement as well as the systems used in dealing with cybercrime must be competent to keep pace with increasingly advanced technological developments.

Keywords: *Customer; Personal data; Banking*

PENDAHULUAN

Pertumbuhan teknologi yang relevan memberikan kemudahan guna mencukupi bermacam kebutuhan tanpa jarak serta waktu. Teknologi dapat memudahkan prosedur, mempersingkat waktu, serta kurangi anggaran dalam melakukan aktivitas. Komitmen transformasi digital pula senantiasa diupayakan Bank Rakyat Indonesia dalam memberikan akses layanan perbankan. Hal ini bisa dilihat pada Tahun 2022 transaksi keuangan menggunakan Internet Banking Bank Rakyat Indonesia mendekati Rp.2.669 triliun atau berkembang lebih dari 2 kali lipat dari rentang waktu tahun sebelumnya, dari jumlah transaksi menjangkau hingga 1,83 miliyar transaksi. Sejalan dengan itu, users Internet Banking pula melesat 68,46% yoy sebagai 23,85 juta users pada Desember 2022 (Narew & Irmawati, 2022).

Imbas positif perkembangan teknologi tidak hanya berlangsung seperti itu, adapula pihak lain dengan itikad buruk mencari profit dengan melakukan kejahatan. Sebagaimana dikatakan dalam penjelasan umum Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik, teknologi informasi kini menjadi pedang bermata dua karena bukan cuma memberikan peran kontribusi peningkatan kesejahteraan, pertumbuhan dan peradaban khalayak, sekaligus selaku sarana efisien tindakan melawan hukum (Iqbal, 2019).

Makin maju kehidupan rakyat, perbuatan melawan hukum juga ikut tumbuh. Indonesia dipandang sebagai negeri dengan index keamanan cyber terburuk di Asia serta dunia. evaluasi itu hasil penelitian oleh Reboot Digital PR Service yang berlandas di Inggris. Mereka mengupas statistik keamanan siber, tercantum unduhan drive-by, phishing, hosting malware, serta pc yang disusupi. Indonesia memangku peringat teratas dengan nilai 82,8 dari 100 serta mendapati sejumlah 643 pc yang terkontaminasi virus, 1.080 phising serta 1.040 memiliki malware.

Di perbankan sendiri terkhusus Bank Rakyat Indonesia Kantor Cabang Watansoppeng sekarang sedang banyak terjadi kejahatan phising dengan modus pesan phising yang mengelabui nasabah seolah itu adalah pesan resmi Bank tersebut.

Istilah "Phising" dikenal pada tahun 1990-an yang berarti "Memancing". Laporan aktivitas phising domain dari Indonesia Anti Phising Data Exchange (IDADX) kuartal 4 (Q4) Tahun 2022, jumlah phising di Indonesia dalam kurun waktu 5 tahun terakhir 42.442 laporan sementara laporan pada Q4 Tahun 2022 ada 6.106 laporan yang terdiri dari bulan Oktober Tahun 2022 2.318 laporan, bulan November Tahun 2022 2.779 laporan, bulan Desember Tahun 2022 1.009 laporan dan industri yang menjadi sasaran serangan phising pada Q4 Tahun 2022 adalah lembaga keuangan sebesar 54% yang selanjutnya posisi kedua sektor eCommerce/Ritel sebesar 31% yang mengalami perubahan dari posisi sebelumnya dimana lembaga pemerintahan berada pada posisi teratas. Jumlah laporan yang diterima IDADX dalam kuartal kedua Tahun 2022 menggambarkan peningkatan pada Q3 Tahun 2022 terdapat 9.428 laporan. Pada kuartal keempat sebanyak 6.106 laporan dimana hal tersebut mengalami pengurangan sebanyak 3.322 laporan phising (Sari, 2021).

Indonesia Anti Phising Data Exchange (IDADX) mencatat 10 nama organisasi/brand yang menjadi target serangan phising pada Q4 2022 dari urutan satu sampai sepuluh diantaranya Morrisons, First National Bank of South Africa, Microsoft, Bank BRI,

Facebook, Malicious Domai, BNP Paribas, British Telecom, Santander, Wells Fargo. Indonesia Anti Phising Data Exchange (IDADX) juga mencatat Indonesia menempati posisi teratas sebagai negara yang menghosting situs phishing domain.id selama Q4 Tahun 2022 yakni pada bulan Oktober 96,81%, bulan November 95,57%, bulan Desember 78,59% dan dilanjutkan pada posisi kedua yaitu United States.

Teknik phising di area perbankan terjadi dengan sistem social engineering. Dimana pelaku menarget pemakai online banking guna medapatkan data kredensial bangking seperti user,password serta sandi OTP. Disamping itu konsumen internet banking Bank Rakyat Indonesia pula amat banyak (Junaedi, 2017). Menurut data yang jumlah konsumen internet banking Bank orang Indonesia Kantor Cabang Watansoppeng sampai pada 27 februari 2023 menyentuh 23.114 pengguna, akibatnya peluang phising pula besar, kerugian yang tidak sedikit karna dapat menghabiskan isi rekening serta sulitnya menemukan pelaku (Patrik & lady, 2022).

Di BRI Kantor Cabang Watansoppeng sendiri khususnya BRI Kantor Cabang Watansoppeng unit Cennae sepanjang tahun 2022 setidaknya telah ada 5 pelaporan yang masuk terkait phising dengan total kerugian mencapai puluhan juta rupiah. Dari informasi Customer service Bank Rakyat Indonesia Cabang Watansoppeng, disampaikan bahwa pihak Bank telah menangani setiap pelaporan nasabah yang masuk sesuai Standar Operasional Prosedur dan kendala yang dihadapi adalah sulit menemukan alur transaksi karena dana nasabah keluar dalam bentuk pembayaran BRIVA.

Dalam KUHP sendiri ketentuan siber masih diatur secara umum, di dalam peraturan hukum Indonesia dikenal asas Lex Specialis derogat legi Generalis yang memiliki arti perundang-undangan atau aturan hukum yang khusus mengesampingkan perundang-undangan atau aturan hukum yang umum, dengan kata lain di Indonesia terdapat Undang-Undang yang mengatur mengenai hukum siber di lingkungan perbankan lebih khusus yaitu Undang-undang Informasi dan Transaksi Elektronik Nomor 11 tahun 2008 yang diubah menjadi Undang-Undang Nomor 19 Tahun 2016, Undang-undang Nomor 10 Tahun 1998 Tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan, Undang-Undang Perlindungan Konsumen Nomor 8 Tahun 1999. Dengan terdapatnya proteksi hukum untuk konsumen, konsumen akan merasa nyaman bila terjadi penyalahgunaan data pribadi miliknya (Triputri, Mofea, Yulviani & Pratama, 2023).

Selain itu ada juga, Peraturan Otoritas Jasa Keuangan, dan berbagai aturan lainnya yang dibutuhkan untuk mencegah cybercrime. Regulasi hukum terkait kejahatan sibertelah ada, namun kejahatan ini juga tetap merajalela sehingga dari permasalah diatas diperlukan penelitian untuk mengetahui bagaimana perlindungan hukum nasabah terkait maraknya kejahatan cyber jenis phising pencurian data pribadi yang terjadi khususnya di wilayah Bank Rakyat Indonesia Kantor Cabang Watansoppeng.

METODE PENELITIAN

Berdasarkan rumusan masalah dan tujuan penelitian, dapat ditentukan bahwa pendekatan yang digunakan dalam penelitian ini adalah penelitian hukumempiris atau disebut dengan penelitian lapangan yaitu mengkaji ketentuan hukum yang berlaku serta apa yang terjadi dalam kenyataan di masyarakat. Dengan kata lain yaitu suatu

penelitian yang dilakukan terhadap keadaan sebenarnya atau keadaan nyata yang terjadi di masyarakat dengan maksud untuk mengetahui dan menemukan fakta dan data yang dibutuhkan, setelah data yang dibutuhkan terkumpul kemudian menuju kepada identifikasi masalah yang akhirnya menuju pada penyelesain masalah. Menurut (Mukti Fajar dan Yulianto 2010) lokasi penelitian sangat diperlukan bagi penelitian hukum terutama bagi penelitian hukum empiris. Berbeda halnya dengan penelitian hukum yang bersifat normatif yang lokasi penelitiannya jelas dilakukan di berbagai perpustakaan. Lokasi penelitian dalam penelitian hukum empiris harus disesuaikan dengan judul dan permasalahan. Penelitian hukum dengan judul "Perlindungan Hukum Nasabah Terhadap Kejahatan Phising Di Lingkungan Perbankan (Studi Kasus Bank Rakyat IndonesiaKantor Cabang Watansoppeng)" Data dan informasi yang diperlukan dalam penelitian ini akan diperoleh di Wilayah Kantor cabang Watansoppeng yang terletak di Kabupaten Soppeng

PEMBAHASAN

A. Efektivitas Perlindungan Hukum Nasabah Terhadap Kejahatan (pencurian data pribadi) Phising Di Lingkungan Perbankan Wilayah Bank Rakyat Indonesia Kantor Cabang Watansoppeng

Dari hasil penelitian dilapangan diketahui pelaku melakukan phising dengan cara mengirimkan tautan/link untuk mengantarkan korban pada situs palsu yang sengaja dibuat. Tautan/link dikirim melalui e-mail, Telepon, SMS, maupun Chat Phishing kepada korban untuk mendapatkan identitas pribadi korban seperti nama asli, username, password, ataupun nomor rekening. Sesudah memperoleh data itu selanjutnya dipakai buat membuka akses data yang sungguh berarti semacam sarana internet banking korban. Jelas tidak mungkin bila pelaku hanya sekedar mencuri data saja namun berkeinginan mencuri tabungan nasabah (Lumakto & Dewi, 2021).

Beberapa modus phishing yang lain diantaranya :

1. Informasi perubahan tarif transfer bank dimana pelaku memberikan informasi palsu dan meminta korban mengisi data rahasia seperti User ID, PIN,OTP, Password, CVC,CVV dan m-Token
2. Layanan konsumen palsu yang mengatasnamakan Bank, mengarahkan korban ke website palsu dan mencuri data rahasianya
3. Tawaran menjadi nasabah prioritas dimana pelaku menawarkan promo upgrade dengan berbaggai hadiah menarik, lalu meminta data rahasia korban
4. Tawaran menjadi agen laku pandai dimana pelaku menawarkan jasa untuk menjadi agen laku pandai lalu meminta korban mentransfer uang untuk mendapatkan mesin EDC.

Informasi oleh nasabah Bank Rakyat Indonesia Kantor Cabang Watansoppeng, Ibu Ismhayantiyang berprofesi sebagai seorang guru, pengguna Internet Banking. Beliau mendapatkan pesan dari nomor yang tidak dikenal dengan gambar profil tertulis Bank Rakyat Indonesia, Isi pesan tersebut menerangkan bahwa IbuIsmhayanti menjadi pemenang undian berhadia di Bank Rakyat Indonesia. Untuk informasi lebih jelas beliau diminta mengklik link tautan yang didalamnya meminta beberapa data pribadi. Karna kurangya pengetahuan Ibu Ismhayanti terkait modus Kejahatan Phishing membuat Ibu Ismhayanti Mengalami Kerugian sejumlah Rp. 29,000,000.00. setelah

notifikasi uang keluar dari rekeningnya baru beliau menghubungi kenalannya di salah baru BRI Unit dan dikonfirmasi transaksi tersebut adalah penipuan.

Terkait dengan kejahatan siber (phising), perlu diingat bahwasanya sifat dari kejahatan ini adalah anonymity. Media siber (internet) memberikan kemudahan bagi pelaku karena pada hakikatnya pelaku tidak mudah terungkap atau terdeteksi dan ditelusuri, dan menggunakan ruang-ruang chatting, facebook, maupun forum diskusi terbuka lainnya.

Seperti yang dialami nasabah Ibu Nurmatia merupakan Nasabah Bank Rakyat Indonesia Cabang Watansoppeng. Ibu Nurmatia juga merupakan seorang guru yang berusia 53 Tahun. Pada salah satu Group Whatssapp Ibu Nurmatia, ada anggota group yang mengirim link undangan pernikahan. Link yang di kirim oleh salah satu anggota group tersebut adalah juga merupakan pesan terusan. Ibu Nurmatia setelah membuka link dari pesan itu semacam mendownload file APK. Tidak berselang lama ada satu lagi orang anggota group memperingatkan untuk tidak mengunjungi link undangan karna dapat mendonwload file APK. Ini merupakan modus phising Via APK yang mana jika file APK itu terdownload di HP seseorang, semua data di HP tersebut dapat di kendalikan oleh orang lain dan dapat mengurus isi saldo rekening seperti yang sedang marak di beritakan saat ini.

Setelah membaca larangan dari temannya, ibu Nurmatia panik dan segera mengunjungi customer service Bank Rakyat Indonesia dan menceritakan masalahnya. Customer service kemudian mengambil langkah, mengecek mutasi rekening ibu Nurmiati yang ternyata masi sesuai saldo sebelumnya lalu melakukan pemblokiran sementara terhadap saldo tersebut atas permintaan ibu Nurmatia. Kemudian customer service membantu nasabah untuk menghapus file APK yang telah terdownload. Customer service menerangkan bahwa saldo nasabah aman dikarenakan Ibu Nurmatia tidak menggunakan Internet Banking di Smartphone nya, sehingga rekeningnya tidak bisa dikendalikan oleh pelaku dan customer service juga berterimakasih karna Ibu Nurmatia telah sigap melakukan pelaporan. Namun karna banyak anggota di group tersebut ibu Nurmatia menjadi khawatir kemungkinan teman-temannya telah mendownload link file APK karna kurangnya pengetahuan tentang bahaya file APK tersebut dan mengira bahwa itu adalah betul undangan pernikahan anak dari salah satu anggota group. Customer service Bank Rakyat Indonesia kemudian menyarankan untuk memberikan informasi ke groupnya untuk segera menghapus file APK yang terlanjut terdownload lalu melakukan pengecekan mutasi rekening, megubah user dan password untuk mengamankan saldo rekening.

Beberapa langkah – langkah yang dilakukan pelaku kejahatan phishing sebagaimana pengalaman Ibu Lisda yang pernah mendapatkan pesan phishing dengan modus perubahan tarif administrasi dari Rp. 8.000 per bulan menjadi Rp. 150.000 per bulan yang membuat nasabah tidak berfikir panjang kemudian mengakses link yang mana merupakan link palsu sebagai pernyataan tidak setuju untuk kenaikan tarif administarsi.

1. Pesan link palsu masuk melalui WA (WhatsApp) kepada calon korban yang telah menjadi sasaran.

2. Dalam pesan tersebut berisi mengenai perintah permintaan informasi yang bersifat personal seperti user id, pin atau nomor kredit.
3. Tidak hanya memberikan pesan singkat kepada korban, para pelaku kejahatan phishing juga memberikan batas waktu untuk mengirimkan data informasi korban yakni satu kali 24 jam, apabila tidak segera mengirimkan data tersebut maka akan ada konsekuensi buruk pada korban yakni dianggap menyetujui perubahan kenaikan tarif administrasi Bank sebesar Rp.150.000/bulan.
4. Korban yang tidak berpikir Panjang maka akan menyerahkan data personalnya kepada para penjahat. Dari data tersebut maka akan disalahgunakan oleh penjahat.

Serangan phising menarget pengguna internet banking biasanya disebarkan melalui WhatsApp. WhatsApp merupakan aplikasi pada selular dengan basic sama blackberry messeger, merupakan aplikasi pesan lintas platform dimana kita dapat bertukar pesan secara gratis. Sehingga cara menghindarkan serangan kejahatan phising mesti dipahami orang lain yang tidak mempunyai hak masuk pada akun internet banking orang lain. Perbankan merupakan salah satu sektor yang sering menjadi eksploitasi para phisher dan kejahatanini tidak hanya mengakibatkan kerugian nasabah saja sebagai korban, tapi juga pihak perbankan mengalami kerugian berupa kepercayaan (Djanggih & Qamar, 2017).

Adapun Prosedur saat nasabah akan menggunakan buku rekening dan fasilitas internet banking di Bank Rakyat Indonesia Kantor Cabang Watansoppeng adalah wajib menggunakan e-KTP dan data NIK dapat diakses melalui database dukcapil, bagi yang belum memiliki e-KTP boleh diganti surat pengganti KTP elektronik serta bukti identitas pendukung seperti SIM, Kartu Pegawai, KTP atau Paspor, Mengisi formulir permohonan fasilitas rekening (FR 01). Formulir permohonan itu berisi data nasabah antara lain:

1. Nama nasabah atau perwakilan nasabah dengan menyertakan surat kuasa.
2. Jenis identitas kartu tanda penduduk ataupun passport dilampiri Izin Tinggal Tetap (KITAP) diberikan kepada orang asing pemegang visa tinggal terbatas dan orang asing pemegang visa terbatas yang telah tinggal di Indonesia sekurang-kurannya lima tahun berturut-turut terhitung sejak tinggal diberikannya izin tinggal terbatas.
3. Nomor Identitas: umumnya berisi nomor kartu tanda penduduk.
4. Alamat nasabah internet banking sesusai identitas nasabah.
5. Nomor rekening yang akan dimintakan permohonan penambahan internet banking.
6. Fasilitas yang diminta pilih e-banking (internet banking) Dan lainnya tentang transaksi otomatis, pernyataan nasabah sampai yang terakhir tanda tangan pemohon fasilitas internet banking dengan disertakan materai Rp 6.000,-

Surat pernyataan lainnya yang harus diisi atau di tanda tangani oleh nasabah sebelum mendapatkan fasilitas internet banking saat pembuatan rekening yang berisi: Yang bertandatangan dibawah ini, saya selaku Nasabah PT. Bank Rakyat Indonesia (Persero) Tbk. menyatakan.

a. Pihak Bank BRI telah memberikan informasi yang jujur, akurat, jelas dan tidak menyesatkan terkait dengan syarat ketentuan produk Bank yang saya gunakan termasuk dan tidak terbatas pada manfaat, resiko dan biaya atas produk/layanan tersebut, dan saya menyatakan mengerti dan menyetujui atas penjelasan Pihak Bank BRI tersebut.
b. Akan mempergunakan dengan tikad baik rekening, buku tabungan, Kartu *ATM,* fasilitas e-banking dan saluran e-channel serta fasilitas perbankan lainnya yang diberikan kepada saya dan tidak menyalahgunakan fasilitas perbankan yang diberikan kepada saya untuk melakukan tindakan melawan dan/atau melanggar hukum.
c. Akan menjaga, menyimpan serta tidak menyerahkan buku tabungan, Kartu *ATM* termasuk fasilitas e-banking dan saluran e-channel serta fasilitas perbankan lainnya yang diberikan kepada saya dan terkait dengan rekening saya kepada pihak lain.
d. Apabila terjadi kehilangan buku tabungan dan/atau Kartu *ATM* termasuk dan/atau transaksi yang tidak wajar atas rekening saya yang menggunakan fasilitas e-banking dan saluran e-channel serta fasilitas perbankan lainnya yang saya gunakan maka saya akan segera melaporkan kepada pihak Bank BRI.

Saya sudah membaca surat pernyataan ini dan memahami penjelasan Customer Service terkait pembukaan rekening beserta fasilitas yang diberikan oleh Bank BRI termasuk cara penggunaan, resiko dan manfaatnya.Apabila dikemudian hari saya melakukan pelanggaran kegiatan tersebut diatas, maka saya bersedia menerima segala konsekuensi hukum maupun konsekuensi lainnya atas pelanggaran tersebut dan melepaskan Pihak Bank BRI dari segala tuntutan.

Dalam memitigasi resiko kejahatan ciber perlindungan yang diberikan oleh Bank Rakyat Indonesia Kantor Cabang Watansoppeng terdiri dari dua tahapan pertama adalah perlindungan dalam rangka pencegahan terjadinya phishing pada nasabah Bank Rakyat Indonesia Kantor Cabang Watansoppeng (perlindungan preventif) dan yang kedua adalah perlindungan ketika nasabah Bank Rakyat Indonesia Kantor Cabang Watansoppeng mengalami tindakan phishing (Perlindungan Represif).

Sebagai langkah Preventif sebagaimana tercantum dalam Pasal 4 Undang-Undang perlindungan konsumen, yang menyatakan bahwa bank memiliki kewajiban untuk memberikan pembinaan dan pemahaman bagi nasabah sebagai konsumen sebagai hak dari konsumen (Priliasari, 2019). Selain itu hal selaras juga diatur dalam Pasal 1 ayat (4) Peraturan Otoritas Jasa Keuangan No. 6/POJK.07/2022 Tentang perlindungan konsumen dan masyarakat di sektor jasa keuangan, perlindungan konsumen dan masyarakat adalah upaya untuk memberikan pengetahuan dan pemahaman atas produk dan/atau layanan Pelaku Usaha Jasa Keuangan (PUJK) yang akan digunakan atau dimanfaatkan oleh Konsumen dan/atau masyarakat, dan upaya memberikan kepastian hukum untuk melindungi konsumen dalam pemenuhan hak dan kewajiban konsumen di sektor jasa keuangan.

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).

Potensi terjadinya tindakan phishing merupakah jenis dari risiko operasional. Risiko Operasional menurut Pasal 1 Butir 7 Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum merupakan risiko akibat ketidakcukupan dan/atau tidak berfungsinya proses internal, kesalahan manusia, kegagalan sistem, dan/atau adanya kejadian-kejadian eksternal yang mempengaruhi operasional bank (Nurapiah, 2019). Michel Crouhy, Dan Gali dan Robert Mark mendefinisikan risiko operasional sebagai risiko yang berkaitan dengan operasional bisnis yang meliputi 2 komponen risiko. Pertama yaitu kegagalan operasional atau risiko internal yang terdiri dari risiko yang bersumber dari sumber daya manusia, proses dan teknologi. Kedua yaitu risiko strategi operasional atau risiko eksternal yang berasal dari faktor antara lain politik, pajak, regulasi, masyarakat dan kompetisi. Dengan potensi terjadinya resiko ini sehingga bank patut menjalankan suatu manajemen resiko guna kurangi resiko yang dapat merugikan nasabah.

Berdasarkan Pasal 53 ayat (1) POJK Nomor 11/PJOK.03/2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum, menyatakan bahwa bank wajib melaksanakan sistem pengendalian intern secara efektif dalam penyelenggaraan teknologi informasi. 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*, serta *bertanggung jawab* terhadap beroperasinya sistem elektronik berjalan sebagaimana mestinya (Saragih, Budhijanto & Somawijaya, 2020).

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 (Diab, 2014).

Setiap Pekerja Bank Rakyat Indonesia Kantor Cabang Watansoppeng secara aktif memberikan Edukasi security awareness kepada seluruh nasabah mengenai tips bertransaksi yang aman melalui internet banking melalui platform media sosial seperti official account twitter, email messaging, status Whatsapp, Instagram, Youtube, Facebook, media cetak dll dengan tujuan agar nasabah dan masyarakat luas mengetahui tentang bahaya penipuan phishing. Edukasi tersebut berisi :

1. Menghimbau kepada nasabah untuk waspada kepada segala bentuk modus penipuan dan kejahatan perbankan;
2. Abaikan pesan dari nomor yang tidak dikenal dan mencurigakan;
3. Channel resmi BRI sudah terverifikasi (centang hijau);
4. Jangan mengklik link dari sumber yang tidak terpercaya, jika sudah klik link palsu segera merubah user, password serta PIN;

5. Mengunduh aplikasi internet banking seperti BRImo melalui Playstore/Appstore;
6. Pastikan tidak memberikan data pribadi kepada siapa pun seperti PIN, Password, kode OTP, kode CVC/CVV dan M-token.

Bank Rakyat Indonesia Kantor Cabang Watansoppeng juga melakukan edukasi kepada nasabah nya melalui cara yang pasif, dengan memberikan kesempatan kepada nasabah untuk bertanya atau melakukan konfirmasi langsung kepada pihak pihak Bank apabila menemukan hal yang ganjal pada simpanannya dan nasabah dapat langsung menghubungi customer service Bank Rakyat Indonesia Kantor Cabang Watansoppeng.

Dalam management resiko, Bank BRI menyediakan layanan pengaduan atau call center di nomor 14017 sebagai langkah pertama apabila nasabah merasa mengalami tindakan phishing. ataupun secara langsung mendatangi unit kerja Bank Rakyat Indonesia Kantor Cabang Watansoppeng. Bank Rakyat Indonesia Kantor Cabang Watansoppeng juga menghimbau agar nasabah untuk hanya membuat laporan melalui satu jalur saja agar tidak menimbulkan laporan ganda.

Bank Rakyat Indonesia memiliki divisi khusus yang bertugas menangani dan menyelesaikan terkait pengaduan nasabah, yaitu Divisi Layanan Contact and Center (Divisi LCC). Dalam penanganan dan penyelesaian pengaduan nasabah Bank Rakyat Indonesia memiliki Standar Operasional dan Pedoman (SOP) tentang Pengelolaan Pengaduan Nasabah, yaitu Surat Keputusan NOKEP S.1051- DIR/LCC/12/2016 tentang Prosedur Penyelesaian Pengaduan Nasabah PT Bank Rakyat Indonesia (Persero) Tbk.

Keberadaan divisi Layanan Contact and Center sebagai divisi khusus yang bertugas menangani dan menyelesaikan pengaduan nasabah. Setelah nasabah menyampaikan pengaduan melalui call center Bank Rakyat Indonesia, agent call center Bank Rakyat Indonesia akan mengeskalasi laporan nasabah tersebut kepada back office Divisi Layanan Contact and Center (Divisi LCC). Kemudian oleh Divisi LCC akan dibuatkan trouble ticket atau laporan, yang kemudian laporan tersebut akan diteruskan ke bagian investigasi divisi Layanan Contact and Center.Kemudian ketika laporan sudah sampai pada bagian investigasi divisi Layanan Contact and Center., maka langkah selanjutnya yang dilakukan oleh Bank Rakyat Indonesia adalah melakukan analisa dan investigasi tehadap pengaduan nasabah.

Proses investigasi dilakukanuntuk mencari tau apakah tindakan phishing yang dialami oleh nasabah merupakan akibat kesalahan nasabah sendiri atau kesalahan dari Bank Rakyat Indonesia (Asmara, Riduan , & Priyadi, 2020). Proses analisa dan investigasi dilakukan oleh Bank Rakyat Indonesia dengan melihat rekening koran dan pola transaksi nasabah. Bank Rakyat Indonesia juga memiliki parameter serta kriteria menentukan sebab terjadinya phising. Dalam hal penyelesaian penanganan pengaduan nasabah, Bank Rakyat Indonesia menetapkan Service Level Agreement (SLA) yaitu maksimal 20 puluh hari kerja.

Dalam memastikan kebenaran proses investigasi, Bank Rakyat Indonesia dapat memperpanjang proses penyelesaian pengaduan nasabah paling lama 20 hari kerja berikutnya, dan perpanjangan ini akan diinformasikan secara tertulis kepada nasabah. Kemudian pihak Bank BRI akan menyampaikan hasil dari penyelesaian pengaduan kepada nasabah yang bersangkutan melalui sarana telepon, e-mail, ataupun surat. Dalam menjaga agar proses penyelesaian pengaduan nasabah tidak melebihi jangka

waktu yang ditentukan, maka bagian investigasi memiliki pengawas internal yang disebut sebagai bagian customer respond, yang bertugas untuk mem foll up agar proses penyelesaian pengaduan konsumen di Bank BRI tidak melebihi SLA.

Apabila dalam proses investigasi Bank BRI menemukan bahwa terjadinya tindakan phishing merupakan kelalaian dan kesalahan nasabah, maka sepenuhnya menjadi tanggung jawab nasabah. Kelalaian yang dilakukan oleh nasabah berupa kelalaian memberikan PIN maupun password pada akun pelaku, walaupun Bank Rakyat Indonesia Kantor Cabang Watansoppeng sudah memberikan edukasi terkait hal tersebut. Sehingga dapat dikatakan terjadinya phishing ketidak hati-hatian nasabah. Dalam hal ini Bank Rakyat Indonesia tidak dapat memberikan ganti rugi, karena hal tersebut bukan merupakan kesalahan Bank Rakyat Indonesia. Kemudian terdapat perlindungan terhadap nasabah jika keadaan yang tidak diinginkan diatas yang telah terjadi dan merugikan nasabah, sehingga diperlukan adanya upaya dalam menyelesaikan permasalahan tersebut. Perlindungan yang bertujuan untuk menyelesaikan masalah disebutperlindungan represif diberikan ketika perlindungan secara preventif tidak dapat menghindarkan nasabah dari kejahatan phishing.

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. Bank sebagai pelaku usaha nasabah mempunyai kewajiban menyampaikan permintaan maaf serta menawarkan ganti rugi (redress/remedy) atau perbaikan produk dan/atau layanan, apabila pengaduan konsumen benar sebagai akibat penggunaan, pemakaian dan pemanfaatan barang dan/atau jasa yang diperdagangkan. atas kerugian konsumen yang timbul karna kesalahan dan/atau kelalaian, pengurus, pegawai pelaku usaha jasa keuangan dan/atau pihak ketiga yang bekerja untuk kepentingan pelaku usaha jasa keuangan. Akan tetapi ganti rugi tersebut tidak berlaku jika bank bisa membuktikan terjadinya phishing merupakan kelalaian dari 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, dalam Pasal 42 ayat (1) POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan menyatakan bahwa Dalam hal layanan pengaduan konsumen oleh POJK tidak tercapai kesepakatan, konsumen dapat melakukan penyelesaian sengketa diluar pengadilan atau melalui 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 52 Nomor 6/POJK.07/202 Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan.

Berikut akan disajikan analisis data gambaran efektivitas perlindungan hukum terhadap phishing berdasarkan sekor angket:

Pada bagian ini akan menguraikan pesan dan media yang digunakan dalam kejahatan phising.

Tabel 1. Tanggapan Responden Tentang Kerentanan Kejahatan Pencurian Data

Pernah Menerima Pesan	Frekuensi	Persentase
YA	36	90
TIDAK	4	10
TOTAL	40	100

(Sumber : data tahun 2023)

Penelitian ini menunjukkan tingginya kerentanan masyarakat terhadap kejahatan pencurian data pribadi (phising), yaitu sebanyak 90% atau 36 responden pernah menerima pesan phising.

Tabel 2. Tanggapan Responden Media Komunikasi Yang Digunakan

Media Phising	Frekuensi	Persentase	Mengalami Kerugian	Persentase
Chat/Telepon	28	70	8	20
Sms	8	20	-	-
Email	-	-	-	-
Total	36	90	8	20

(Sumber : data tahun 2023)

Media komunikasi yang paling banyak digunakan dalam penipuan adalah jaringan seluler (telepon/WhatssApp) (70%)28 org yang sifatnya sangat mudah, murah, dan merupakan fitur mendasar sehingga jangkauannya bisa sangat luas dan Media terbanyak selanjutnya adalah SMS (20%) 8org.

Meski demikian, lebih dari separuh responden 70% atau 28 org yang menjadi korban penipuan menyatakan bahwa mereka "tidak mengalami kerugian". Sementara itu,korban yang menyatakan mengalami kerugian materi berjumlah 20% atau 8 orng responden.

Tabel 3. Sikap Responden Terhadap Pesan Phising

Sikap Terhadap Pesan	Frekuensi	Persentase
menceritakan kepada keluarga atau teman	19	47,5
tidak melakukan apa-apa	10	25
melaporkan ke bank terkait	9	22.5
melaporkan kepadakepolisian	2	5

(Sumber : data tahun 2023)

Dari seluruh korban penipuan tersebut, respons atau tindakan terbanyak yang mereka lakukan adalah menceritakan kepada keluarga atau teman (47,5%) 19 org, tidak melakukan apa-apa (25%) 10 org, melaporkan ke bank terkait (22.5%) 9 org, dan melaporkan kepada kepolisian (5%) 20rng.

Melaporkan kepada bank terkait merupakan tindakan yang sebaiknya segera dilakukan saat mendapat pesan phising agar kita dapat segera mengamankan saldo di rekening sementara waktu.

Laporan ke polisi jarang dilakukan oleh korban kejahatan siberpadahal merupakan cara terbaik,sangatlah penting karena bisa menjadi contoh bagi orang lain yang mungkin mengalami kejadian serupa dan agar kedepan juga bisa ditemukan cara pencegahan atas tindakan kejahatan tersebut.Namun mudahnya melakukan pelaporan terhadap suatu kasus tidak sebanding dengan mudahnya penanganan dan penindakan oleh pihak bank terkait maupun kepolisian. Kedua pihak ini diperlukan sama-sama menjadi lebih pintar dan paham mengenai undang-undang dan sistem teknologi dalam menangani kejahatan siber. Selain itu peran serta masyarakat juga dibutuhkan agar lebi hari-hari dengan penggunaan teknologi khususnya berkaitan dengan data pribadi.

Tabel 4. Kategori Efektifitas Perlindungan Hukum Nasabah

No	Kategori Jawaban	Frekuensi	Persentase
1	**Ya**	16	40
2	**Tidak**	24	60
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Dari tabel tersebut dapat diketahui bahwa mayoritas responden menilai penanganan pengaduan tidak efektif sebesar 60% responden, sedangkan sebesar 40% beranggapan penanganan pengaduan sudah baik. Data ini membuktikan bahwa dalam penaganan pelaporan kejahatan di sektor perbankan masih perlu di tingkatkan. Yang menjadi celaadalahprofesional penegak hukum yang sektor perbankan yang belum mempuni yaitu pegawai bank itu sendiri sebab kenyataannya jika terjadi adanya suatu tindak kejahatan transaksi elektronik pada sektor perbankan sering kali hal tersebut hanya dilakukan suatu himbauan saja bukan ditindak tegas secara jelas hal ini disebabkan belum di dukung oleh sarana prasarana yang lebih canggih agar bisa melacak alur transaksi kejahatan phishing untuk mengungakap locus dan tempus dicti .

Secara spesifik ada 3 dimensi yang digunakan penulis dalam menjelaskan efektivitas perlindungan hukum nasabah oleh bank terhadap kejahatan phising yaitu : kejelasan informasi tentang produk dan layanan, kepercayaan terhadap perbankan, dan sistem keamanan perbankan yang baik. Penulis paparkan sebagai berikut :

1. Dimensi kejelasan informasi produk dan layanan

Tabel 5. Tanggapan Responden Pihak bank telah memberikan informasi lengkap terkait produk, jasa, prosedur pengaduan nasabah dan pentingnya menjaga data pribadi

Jawaban	Frekuensi	Persentase
Ya	26	65
Kurang	10	25
Tidak	4	10
Total	**40**	**10**

(Sumber : data angket tahun 2023)

Data menunjukkan bahwa kebanyakan responden masuk dalam tingkat kategori menperoleh informasi yang lengkap dari pihak bank sebesar 65% reponden, sedangkan sebesar 25% masuk dalam kategori kurang mendapatkan informasi lengkap dan sisanya 10% tidak mendapatkan informasi lengkap.

2. Kepercayaan terhadap perbankan

Tabel 6. Tanggapan Responden Pihak bank tidak menyalahgunakan data pribadi nasabah tanpa izin

Jawaban	Frekuensi	Persentase
Ya	39	97,5
Tidak	1	2,5
Total	**40**	**100**

(Sumber : data angket tahun 2023)

Dari hasil respon yang diperoleh 97,5% responden setuju bahwa kejahatan phishing bukan dikarenakan penyalahgunaan data pribadi nasabah yang dilakukan tanpa izin dari pihak bank dan responden percaya terhadap perbankan yang menyimpan data pribadi mereka.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjelaskan Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara sendiri atau di kombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik. Contoh data pribadi yang bersifat umum antara lain: nama lengkap, alamat, tempat tanggal lahir, nomor telepon, kewarganegaraan, agama, status perkawinan, jenis kelamin. Sementara data pribadi yang bersifat spesifik antara lain :nomor rekening, saldo rekening, mutasi rekekning, nomor kartu debit, dan data kartu kredit.

3. Sistem keamanan perbankan yang baik

Tabel 7. Tanggapan Responden Pihak bank memiliki sistem keamanan yang baik

Jawaban	Frekuensi	Persentase
Ya	14	35
Tidak	26	65
Total	**40**	**100**

(Sumber : data angket tahun 2023)

Dari data, 65% responden menilai bahwa sistem keamanan Bank Rakyat Indonesia belum baik dan 35% menilai sudah baik artinya responden menganggap perlunya dilakukan peningkatan pada sistem keamanan. Wawancara dengan nasabah korban Ibu Ishmayanti, beliau menyadari penipuan terjadi akibat beliau yang kurang berhati-hati namun beliau sangat mengharapkan uangnya kembali saat melakukan pelaporan di customer service. Ibu Ishmayanti sangat mengharapkan di unit kerja Bank Rakyat Indonesia terdapat sistem yang mampu menemukan alur transaksinya kemudian menemukan pelaku agar dapat diproses sebagaiamana ketentuan hukum yang ada.

Faktor-faktor yang mempengaruhi efektivitas perlindungan hukum nasabah terhadap kejahatan phising di lingkungan perbankan wilayah Bank Rakyat Indonesia Kantor Cabang Watansoppeng.

Efektivitas strategi penanggulangan kejahatan perlu mempertimbangkan factor-faktor penyebab kejahatan. Kapan kondisi-kondisi tertentu secara konsisten dapat dihubungkan dengan kejahatan.

1. Faktor Pengetahuan

Tabel 8. Tanggapan responden Berdasarkan indikator, apakah anda mengetahui terkait kejahatan pencurian data pribadi (Phishing) sebelum banyaknya edukasi tentang bahaya phising.

No	Kategori Jawaban	Responden	Persentase
1	**Sangat tidak tau**	6	15
2	**Tidak tau**	25	62,5
3	**Kurang tau**	5	12,5
4	**Cukup tau**	4	10
5	**Sangat tau**	0	0
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Berdasarkan data, sebanyak 15% atau 6 peserta menjawab sangat tidak tau, 62,5% atau 25 peserta menjawab tidak tau,12,5% atau 5 peserta menjawab kurang tau dan 10% atau 4 peserta menjawab cukup tau.

Sampai saat ini kesadaran hukum masyarakat Indonesia dalam merespon aktivitas cybercrime masih dirasa kurang. Hal ini disebabkan oleh kurangnya pengetahuan dan pemahaman (lack of information) masyarakat terhadap jenis kejahatan cybercrime sehingga penanggulangan phishing mengalami kendala dalam penataan hukum dan pengawasan hukum.

Bagian yang terpenting dari masyarakat yang menentukan penegakan hukum adalah kesadaran hukum masyarakat. Semakin tinggi tingkat kesadaran hukum masyarakat, maka akan semakin memungkinkan penegakan hukum yang baik. Sebaliknya semakin rendah tingkat kesadaran hukum masyarakat, maka akan semakin sukar untuk melaksanakan penegakan hukum yang baik. Kesadaran hukum antara lain meliputi: Pengetahuan tentang hukum, Penghayatan fungsi hukum dan ketaatan terhadap hukum.

Jika masyarakat memiliki pemahaman yang benar baik secara langsung maupun tidak langsung masyarakat akan membentuk pola penataan. Pola penataan ini dapat berdasarkan karna ketakutan akan ancaman pidana atau pola penataan yang tumbuh atas kesadaran sendiri sebagai masyarakat hukum. Dalam upaya pengawasan peran masyarakat sangat penting. Ketika masyarakat mengalami kurang pengetahuan dan pemahaman (lack of information) peran masyarakat akan menjadi mandul. Misalnya dalam masyarakat yang kurang pengetahuan dan pemahaman (lack of information) datang mahasiswa membawa computer lalu memesan barang mewah menggunakan carding. Karna masyarakat tidak mengetahui sehingga tidak curiga bahkan sebaliknya cenderung terkesan.

Lain halnya dengan delik konvensional seperti pencurian masyarakat umum telah mengetahui sehingga dapat dicurigai melakukan pencurian, masyarakat dapat mengantisipasinya.

Tabel 9. Tanggapan responden ancaman phishing membuat saya ragu menggunakan fasilitas perbankan

No	Kategori Jawaban	Frekuensi	Persentase
1	**Ya**	21	52,5
2	**Tidak**	19	47,5
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Perasaan takut menggunakan fasilitas perbankan juga menunjukkan kurangnya pengetahuan terkait penyebab terjadinya kejahatan phishing yang disebabkan oleh kurangnya kehati-hatian nasabah dalam menjaga data rahasianya.

Tabel. 10. Tanggapan responden membedakan link resmi dan tiruan

No	Kategori Jawaban	Frekuensi	Persentase
1	**Ya**	9	22,5
2	**Tidak**	31	77,5
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Berdasarkan data tersebut, sebesar 77,5% responden tidak bias membedakan alamat tautan/link resmi dan sebesar 22,5% dapat membedakan alamat lautan resmi.

2. Faktor Sarana Prasarana

Tabel 11. Tanggapan responden memperoleh informasi yang saya perlukan di internet

No	Kategori Jawaban	Frekuensi	Persentase
1	**Ya**	31	77,5
2	**Tidak**	9	22,5
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Dari data 77,5% responden memiliki kemudahan akses internet yang ditunjang oleh jangkauan jaringan yang baik dan sarana yang digunakan seperti handphone dan PC yang mayoritas orang sudah memilikinya. Sementara 22,5% responden menjawab tidak dikarenakan sebagian dari wilayah Bank Rakyat Indonesia Cabang Watansoppeng adalah daerah gunung yang sulit jangkauan internet dan tingkat pendidikan masyarakat yang masi rendah yang terbatas dalam menggunakan alat komunikasi.

Berdasarkan hasil survey Asosiasi Pemyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia mencapai 215,63 juta orang pada periode tahun 2022 hingga 2023 ini setara dengan 78,19% dari total populasi indonesia sebesar 275,77 juta jiwa dan rata-rata durasi penggunaan internet di Indonesia selama 7 jam 42 menit pada kuartal III 2022. Sehingga yang harus dijaga adalah kebijakan dan kecermatandalam menggunakan fasilitas internet.

3. Faktor Psikologi

Tabel 12 Tanggapan responden berfikir panjang saya biasa membuka alamat link yang tidak saya ketahui

No	Kategori Jawaban	Frekuensi	Persentase
1	**Ya**	12	30
2	**Tidak**	28	70
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Dari data ada 30% responden yang berprilaku impulsive terhadap suatu yang tidak diketahui, sementara 70% responden menjawab tidak. Korban memiliki peran dalam terjadinya kejahatan Phishing yakni kurang teliti dan tidak berfikir panjang saat menggunakan internet.

4. Faktor Budaya Privasi berjejaring social

Tabel 13. Tanggapan responden jika ada yang menghubungi saya, begitu meyakinkan mengatakan dari perbankan dan meminta verifikasi data, saya memberikan verifikasi tersebut

No	Kategori Jawaban	Frekuensi	Persentase
1	**Ya**	12	30
2	**Tidak**	28	70
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Berdasarkan data, terdapat 12 responden yang memiki awareness atau kesadaran yang rendah akan adanya kejahatan cyber.

Tabel 14. Tanggapan responden menyimpan data pribadi seperti nomor handphone dan alamat di profile media social

No	Kategori Jawaban	Frekuensi	Persentase
1	**Ya**	17	42,5
2	**Tidak**	23	57,5
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Faktor rendahnya kesadaran menjaga privasi dalam menggunakan internet yang lumayan tinggi sangat mempengaruhi keberhasilan kejahatan phishing.

5. Faktor Pendidikan

Tabel 15. Tanggapan res[onden Edukasi bahaya phishing diperlukan untuk mencegah kejahatan phishing

No	Kategori Jawaban	Frekuensi	Persentase
1	**Ya**	37	92,5
2	**Tidak**	3	7,5
	Total	**40**	**100**

(Sumber : data angket tahun 2023)

Dari data tersebut 92,5% responden berpendapat tentang di perlukannya edukasi tentang bahaya phishing dan sisanya 7,5% responden merespon tidak perlu. Hampir mayoritas waktu dalam kehidupan masyarakat saat ini tidak lepas dari penggunaan teknologi digital baik untuk bekerja, belajar maupun bersosialisasi baik itu lewat komputer, handphone, ataupun perangkat lain yang terdapat di kantor ataupun di rumah kita. Interaksi pengguaan teknologi sudah menjadi kebiasaan masyarakat dari bangun tidur sampai tidur lagi.

Risiko kejahatan siber menjadi pengetahuan yang penting untuk diketahui oleh masyarakat. Namun, dalam prakteknya tidak banyak masyarakat di Indonesia memahami hal tersebut, sehingga masih banyak masyarakat ataupun organisasi di Indonesia menjadi korban dari kejahatan siber ini. Hal ini tentu perlu menjadi perhatian kita semua, untuk semakin meningkatkan kesadaran masyarakat mengenai potensi kejahatan siber yang ada, dalam setiap aktivitas kita di ruang digital.Negara Indonesia menduduki peringkat ke 76 dengan nilai index 38.96. Berdasarkan NCSI Indonesia masih memiliki nilai kurang baik untuk banyak aspek, salah satunya terkait dengan pendidikan/literasi.

Keterkaitan antar faktor diatas berjalan dengan sangat erat dan penting untuk dipenuhi untuk tercapainya penegakan hukum yang efektif. pihak bank sebagai penegak hukum utama dalam transaksi elektronik sektor perbankan dan masyarakat akan merasa kegiatan transaksi online yang dilakukannya aman selama dibimbing oleh pegawai bank itu sendiri agar pengetahuan nasabah terkait berbagai kejahatan dunia maya serta pentingnya privasi berjejaring sosial dapat meningkat.

Dengan kondisi Indonesia yang mengutamakan transaksi online dibandingkan dengan transaksi offline saat ini menjadikan justru kasus-kasus kejahatan fraud khususnya fraud phishing menjadi semakin meningkat. Oleh karena itu, pengaturan yang secara khusus mengatur kegiatan transaksi elektronik yang lebih khusus jika terjadinya kejahatan fraud phishing sangat dibutuhkan penambahan kebijakan hukum yang lebih progresif selain dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Aturan-aturan tersebut harus didasarkan juga pada asas-asas yang berlaku pada sistem hukum di Indonesia efektivitas hukum dalam perundang-undangan tersebut dapat berjalan dengan baik. Sebab penerapan Undang-Undang Informasi dan Transaksi Elektronik dalam penegakan fraud phishing di Indonesia masih memiliki faktor kekurangan yang di antaranya adalah:

a. Masyarakat yang menggunakan teknologi secara bebas, yang artinya masyarakat memang benar-benar apatis dan tidak mengenal batasan terhadap larangan yang tercantum dalam Undang-Undang Informasi dan Transaksi Elektronik .
b. Pemikiran dan kemampuan masyarakat Indonesia yang dianggap belum sepenuhnya paham terhadap konsekuensi penggunaan transaksi elektronik. Segala kegiatan transaksi elektronik dianggap sesuatu yang pasti aman sehingga tindakan-tindakan ilegal yang dilakukannya tidak akan terjadi apapun.
c. Undang-Undang Nomor 19 Tahun 2016 tentang perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik belum menjelaskan konsep phising. Perlu dilakukan perubahan kebijakan khususnya

pasal 35 karna mendekati konsep phising tapi beberapa unsur phising tidak dirumuskan dalam pasal 35 sehingga menyebabkan kekaburan norma hukum.

Faktor pelaksana penegak hukum yang kurang tegas dalam menindaklanjuti kasus-kasus transaksi elektronik seperti fraud phishing sehingga tidak menimbulkan efek jera, padahal kejahatan tersebut dapat mengganggu masyarakat

KESIMPULAN

1. Efektivitas perlindungan hukum nasabah terhadap kejahatan phising di lingkungan perbankan Bank Rakyat Indonesia Kantor Cabang Watansoppeng yakni perlindungan hukum preventif telah diterapkan dengan baik. Namun perlindungan hukum represif belum efektif karna masi tingginya tingkat kejahatan dan sulitnya menemukan pelaku disebabkan kecepatan transaksi yang terjadi, pihak bank tidak sembarang memblokir rekening penampungan karna ada prosedur tertentu yang harus dipenuhi, adanya rekening fiktif penampungan mungkin menggunakan identitas korban sebelumnya, pelaku menghapus jejak digital, pelaku bisa berada dimana saja sehingga sulit menerapkan sanksi hukum yang tegas.
2. Faktor-Faktor yang mempengaruhi efektifitas perlindungan hukum nasabah terhadap kejahatan phising di lingkungan perbankan antara lain Faktor pengetahuan tentang phising masih rendah, Faktor sarana dan prasarana, faktor psikologi masyarakat, faktor budaya privasi dan faktor pendidikan dan pemahaman yang rendah sehingga diperlukan edukasi tentang bahaya kejahatan siber.

SARAN

Kesadaran hukum nasabah dalam menjaga data pribadi harus di tingkatkan agar nasabah atau masyarakat dapat terhindar dari kejahatan siber. Kemampuan penegak hukum maupun sistem yang digunakan dalam menangani kejahatan siber harus mempuni untuk dapat mengimbangi perkembangan teknologi yang semakin maju.

DAFTAR PUSTAKA

Asmara, F. T., Riduan, A., & Priyadi, M. P. (2020). Kebijakan dan Implementasi Strategi Anti-Fraud pada Bank Umum. *InFestasi*, *16*(2), 135-147.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journal*, *13*(1), 10-23.

Diab, A. L. (2014). Pembuktian dengan Teknologi Modern dan Teknologi Informasi. *Al-'Adl*, *7*(1), 99-118.

Iqbal, M. (2019). Efektifitas Hukum Dan Upaya Menangkal Hoax Sebagai Konsekuesni Negatif Perkembangan Interkasi Manusia. *Literasi Hukum*, *3*(2), 1-9.

Junaedi, D. I. (2017). Antisipasi Dampak Social Engineering Pada Bisnis Perbankan. *Infoman's*, *11*(1), 1-10.

Lumakto, G., & Dewi, N. K. (2021). Mehamami Modus dan Pencegahan Penipuan Penggalanganan Donasi Online: Understanding Modes and Prevention of Online Donation Fraud. *Jurnal Bimas Islam*, *14*(2), 393-418.

Narew, I., & Irmawati, I. (2022). Analisis Faktor–Faktor Yang Mempengaruhi Minat Masyarakat Dalam Menggunakan Layanan E-Banking Pt Bank Rakyat Indonesia, Tbk. *JURNAL ULET (Utility, Earning and Tax)*, *6*(2), 125-144.

Nurapiah, D. (2019). Manajemen Risiko Operasional Pada Perbankan Syariah Di Indonesia. *EKSISBANK (Ekonomi Syariah dan Bisnis Perbankan)*, *3*(1), 66-73.

Patrik, J., & Lady, L. (2022). Faktor yang Mempengaruhi untuk Menggunakan Mobile Banking dari Internet Banking Terhadap Penggunaan Konsumen Perbankan di Indonesia. *SEIKO: Journal of Management & Business*, *5*(1), 284-299.

Priliasari, E. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online. *Majalah Hukum Nasional*, *49*(2), 1-27.

Saragih, L. K., Budhijanto, D., & Somawijaya, S. (2020). Perlindungan hukum data pribadi terhadap penyalahgunaan data pribadi pada platform media sosial berdasarkan undang-undang republik indonesia nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elek. *JURNAL HUKUM DE'RECHTSSTAAT*, *6*(2), 125-142.

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58-77.

Triputri, D. H., Mofea, S., Yulviani, D., & Pratama, R. (2023). Analisis Yuridis Terhadap Penerapan Sanksi Pidana Bagi Pelaku Penipuan Dalam Transaksi Elektronik Berdasarkan Asas Lex Specialis Derogat Legi Generali Ditinjau Dari Kuhp Dan UU ITE. *Lex Veritatis*, *2*(01), 42-51.