Volume 5 Issue 2 (2024) Pages 721 - 731
Economics and Digital Business Review
ISSN : 2614-851X (Online)

Berita Hoax Terhadap Reputasi Bank

Hanan Salsabila Ruvianti[1], Leonard Adrie Manafe[2]
[1,2] STIE Mahardika Surabaya Program Studi Manajemen dan Akuntansi

Abstrak
Penelitian ini dilatar belakangi oleh banyaknya kasus penipuan *online* yang terjadi khususnya di dunia perbankan. Tujuan dari pembuatan artikel ini yaitu untuk mengetahui bagaimana keterkaitan antara kasus penyebaran berita *hoax* dan modus penipuan terhadap reputasi perbankan serta faktor- faktor yang dapat mempengaruhi reputasi perbankan, mengetahui dampak negatif yang ditimbulkan terhadap nasabah, dan mengetahui tindakan pencegahan yang seharusnya diambil baik oleh nasabah maupun pihak bank agar angka penipuan khususnya di bidang perbankan dapat menurun. Dengan adanya jurnal ini diharapkan dapat menekan angka penipuan menjadi lebih kecil dan meningkatkan *customers awareness*. Penelitian ini dilakukan dengan melibatkan 4 narasumber dengan menggunakan sumber data dari hasil wawancara untuk mendapatkan data yang valid sehingga dapat membantu dalam penyusunan jurnal ini.

Kata kunci : *modus penipuan bank, reputasi perbankan, berita hoax*

✉ Corresponding author :
Email Address : hananslsbl@gmail.com, leo.adriemanafe@gmail.com

PENDAHULUAN

Kemajuan teknologi yang saat ini kita rasakan tentu menghadirkan banyak hal positif yang signifikan bagi penggunanya terutama dalam kemudahan akses yang didapat, melalui internet kita bisa mendapatkan semua informasi yang ingin kita cari dengan cepat dan mudah, hal ini dinilai sangat efisien sehingga dapat meningkatkan produktivitas serta kualitas waktu yang akhirnya dapat digunakan dengan lebih bijak. Berdasarkan data yang yang dirilis oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2022 jumlah pengguna internet di Indonesia adalah sekitar 210 juta orang atau kurang lebih 78,4% dari total penduduk di Indonesia. Masyarakat memiliki berbagai macam kebutuhan untuk penggunaan internet seperti kebutuhan bisnis, hiburan, pendidikan, dan komunikasi. Salah satu kegiatan yang paling sering digunakan adalah penggunaan sosial media (*Instagram, Tiktok, Facebook, Youtube,* dsb) untuk terhubung dan berkomunikasi dengan kerabat atau teman, mencari informasi, serta sekedar mengikuti tren yang sedang berjalan saat ini. Tidak hanya *scrolling* media sosial, namun masyarakat juga gemar

melakukan belanja *online* (Hermawansyah, 2022) karena penggunaan *e-commerce* yang semakin mudah dan memiliki beragam variasi *platform* seperti *Shopee, Tokopedia, BliBli*, dsb (Akbar & Alam, 2020).

Kehadiran teknologi yang semakin maju juga membuka banyak sekali peluang di berbagai bidang salah satunya pada sektor perbankan, sadar akan teknologi yang semakin hari makin berkembang, perbankan terus melakukan inovasi untuk meningkatkan kualitas dan mutu layanan agar nasabah senantiasa dapat melakukan transaksi dengan nyaman dan aman salah satunya dengan menghardikan layanan perbankan digital seperti *mobile banking* yang memungkinkan nasabah untuk mengakses layanan perbankan yang sudah disediakan dimana pun dan kapan pun nasabah membutuhkan. Dengan adanya aplikasi *digital* bank nasabah tidak perlu repot untuk datang ke cabang untuk melakukan transaksi, hal ini dinilai sangat efisien dan dapat menghemat waktu.

Namun hal ini juga tidak lepas dari dampak negatif serta kejahatan yang dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab yang dapat merusak nama baik dari perusahaan dan menyebabkan kerugian materi bagi korban. Kejahatan yang terjadi di internet juga disebut dengan *Cybercrime*. *Cybercrime* adalah suatu tindakan kriminal yang bersifat ilegal dengan memanfaatkan teknologi yang canggih seperti perangkat hingga jejaring internet untuk mendapatkan informasi yang bersifat rahasia atau pribadi (Ramailis, 2020). Tidak hanya meretas data korban, namun *cybercrime* juga melakukan kejahatan seperti pencurian perangkat keras dan perangkat lunak, memanipulasi data, mengubah program secara ilegal, dsb (Saputra, 2022). *Cybercrime* dalam arti sempit merupakan aktivitas mencurigakan ilegal atau melanggar hukum secara langsung dengan menyerang sistem keamanan komputer dan data yang diproses oleh komputer, sedangkan *cybercrime* dalam arti luas, yaitu aktivitas mencurigakan, ilegal atau melanggar hukum terkait dengan sistem atau jaringan komputer (Yanuar, 2021). Salah satu penyebab utama terjadinya *cybercrime* adalah kurangnya kesadaran masyarakat akan keamanan siber. Selain itu, faktor lain seperti kelemahan sistem keamanan dan tingginya nilai aset digital juga mendorong terjadinya *cybercrime*.

Reputasi perbankan menjadi faktor utama yang dapat memberikan banyak keuntungan bagi bank terutama dalam membangun citra positif dan meningkatkan *value* dari perusahaan, meningkatkan kepercayaan nasabah dan menarik nasabah baru untuk bergabung, meningkatkan daya saing bank dan menjadi bank yang unggul diantara yang lain, memudahkan bank dalam mendapatkan dana melalui debitur-debiturnya, dsb. Reputasi perusahaan yang baik dapat terbentuk dari reputasi produk yang baik juga (Keller, 2020). Reputasi bank berhubungan dengan sejarah, kinerja, dan nilai-nilai yang dimiliki oleh bank tersebut (Doney dan Cannon, 2020) dari riwayat perusahaan tersebut dapat dinilai seperti apa hubungan kerja sama antara bank dengan pihak lain seperti nasabah dan pihak ketiga apakah memiliki hubungan yang baik atau tidak yang kemudian masyarakat dapat menilai sendiri reputasi dari perusahaan yang terbentuk berdasarkan pengalaman,keyakinan, dan nilai yang melekat pada bank tersebut (Kasmir, 2021). Risiko reputasi dapat mempengaruhi harga saham dan kapitalisasi pasar bank serta memiliki implikasi jangka panjang terhadap bisnis dan operasional bank (Eka Wahyu, 2023), maka dari itu bank harus dapat memastikan bahwa bisnis yang

dijalankan adalah etis dan bersifat transparan, melakukan pemantauan serta mengelola risiko reputasi dengan baik untuk memastikan reputasi bank tetap baik dan stabil (Kunitsyna, 2023)

Dari beberapa pengertian reputasi perbankan menurut para ahli dapat ditarik kesimpulan bahwa reputasi perbankan dapat diartikan sebagai persepsi yang diberikan oleh publik terhadap bank yang terbentuk berdasarkan pengalaman pribadi, keyakinan dan kepercayaan, kinerja dari bank, kredibilitas serta integritas yang diberikan oleh bank kepada nasabah atau masyarakat. Adapun teori-teori yang berkaitan dengan reputasi perbankan yaitu: a) Teori Sinyal (*Signaling Theory*), teori sinyal adalah langkah-langkah yang dilakukan oleh manajemen perusahaan untuk menunjukkan kredibilitas atau kemampuan kinerja dari perusahaan tersebut (Brigham & Housten, 2023). Pada teori ini dijelaskan bagaimana suatu perusahaan harus memberikan sinyal kepada berbagai pihak melalui laporan keuangan yang bersifat transparan/terbuka, dengan begitu manajemen perusahaan dapat memberikan petunjuk bahwa perusahaan memiliki prospek yang unggul dibanding perusahaan lain. Teori sinyal memiliki fungsi sebagai sarana untuk menyampaikan informasi oleh pihak internal khususnya manajemen kepada para pengguna (*user*) dan dapat dijadikan sebagai acuan untuk mengambil suatu keputusan yang dinilai berdasarkan potensi yang dimiliki suatu perusahaan (Suganda, 2023), b) *Good Corporate Governance (GCG)*, menurut Hery pada jurnal Anak Agung Ayu Astari Fana tahun 2022, GCG menggambarkan strategi untuk merencanakan hubungan baik antara pemegang saham, pengurus perusahaan, kreditur, pemerintah, karyawan, serta pemegang kepentingan intern dan ekstern lainnya yang berurusan dengan hak serta kewajiban mereka untuk memutuskan dan menjalankan arah program serta kinerja perusahaan. GCG memiliki tujuan untuk menambah nilai pemegang saham dalam jangka panjang dan tetap mengawasi kepentingan *stakeholders* (Supriyanto dan Eko, 2022), c) Teori *Stakeholder, stakeholder* merupakan pihak eksternal ataupun internal yang memiliki kepentingan di perusahaan yang dapat mempengaruhi bisnis. Teori *stakeholder* berhubungan antara perusahaan dan *stakeholders* (masyarakat, pemerintah, pemegang saham, konsumen, dsb) yang artinya perusahaan bukan hanya bergerak untuk kepentingan perusahaan namun harus memperhatikan kepentingan *stakeholders* serta memberikan manfaat bagi *stakeholders* (Syeren Al Gista dan Dewi Prastiwi, 2022).

METODELOGI

Jenis penelitian yang digunakan oleh penulis pada jurnal ini adalah penelitian kualitatif. Penelitian kualitatif deskriptif adalah penelitian yang berlandaskan *postpositivisme* digunakan untuk meneliti pada kondisi objek alamiah dimana peneliti sebagai instrumen kunci (Sugiyono, 2022). Menurut Moleong (2022) penelitian kualitatif deskriptif adalah suatu penelitian dimana data-data yang dikumpulkan berupa kata-kata, gambar, dan bukan merupakan angka. Data-data tersebut diperoleh dari hasil wawancara, catatan lapangan, foto atau dokumentasi, catatan, dsb. Penelitian ini menggunakan data yang ada dan kemudian dijelaskan secara lebih rinci dengan tujuan agar dapat memberikan gambaran lengkap mengenai topik yang menjadi pembahasan pada jurnal ini. Pendekatan yang peneliti gunakan adalah pendekatan fenomenologi berdasarkan pengalaman pribadi yang dialami oleh narasumber dengan menggunakan teknik wawancara dan observasi mendalam

untuk mendapatkan data. Dalam jurnal ini yang menjadi informan antara lain : a. *Customer Service,* b. Pimpinan Cabang, c. Bagian Hukum, d. *Frontliner*

No.	Pertanyaan
1.	Apa faktor yang membuat nasabah rawan untuk masuk ke dalam penipuan *online*?
2.	Bagaimana tindakan yang diambil pihak bank dalam menyelesaikan kasus penipuan yang dialami oleh nasabah?
3.	Apakah hukum di indonesia tentang tindak pidana *cybercrime* sudah kuat untuk melindungi konsumen/nasabah?
4.	Apakah perbankan sudah memberikan informasi sekaligus mengedukasi nasabah perihal modus penipuan transaksi *online*?
5.	Bagaimana tingkat keamanan yang diterapkan oleh bank dalam melindungi data nasabah

Tabel pertanyaan wawancara

HASIL DAN PEMBAHASAN

Faktor-faktor yang membuat nasabah masuk ke dalam modus berita hoax

Melalui wawancara yang telah dilakukan kepada pihak internal Bank Centra Asia Tbk diantaranya yaitu pimpinan cabang dan *frontliner* bank sebagai sumber informasi yang membahas mengenai kaitan antara reputasi bank terhadap berita *hoax*, peneliti menemukan bahwa terdapat beberapa faktor yang membuat nasabah dengan mudahnya terjebak untuk mempercayai berita palsu yang mengatasnamakan perbankan yaitu nasabah cenderung gampang untuk mempercayai berita yang tidak jelas sumbernya berasal dari mana dan tidak melakukan verifikasi terkait kebenaran sumber berita kepada instansi yang bersangkutan. Sebagai contoh penipuan dengan modus arisan online atau investasi bodong dengan iming-iming *return* dana yang tinggi serta pemalsuan testimoni yang dilakukan oleh pelaku penipuan, kemudian ada juga modus yang berupa ajakan untuk menjadi nasabah prioritas dengan tawaran yang menggiurkan bagi nasabah yaitu hanya dengan uang Rp. 10.000.000 nasabah sudah bisa upgrade menjadi nasabah prioritas, modus ini mengharuskan nasabah untuk melakukan pengisian data pribadi yang bersifat rahasia yang kemudian digunakan oleh pelaku untuk menguras saldo rekening nasabah. Usia rata-rata yang umumnya tertipu dengan modus seperti ini adalah antara 30-50 tahun.

Kurangnya literasi dan pemahaman nasabah terhadap perkembangan teknologi yang saat ini semakin canggih juga dapat meningkatkan angka penipuan *online*, masyarakat cenderung gampang untuk mempercayai berita palsu yang tersebar di internet tanpa memahami isi dari berita tersebut, berita palsu cenderung mengarahkan nasabah untuk melakukan pengisian data pribadi yang bersifat rahasia, bahkan di beberapa kasus para pelaku penipuan secara terang-terangan

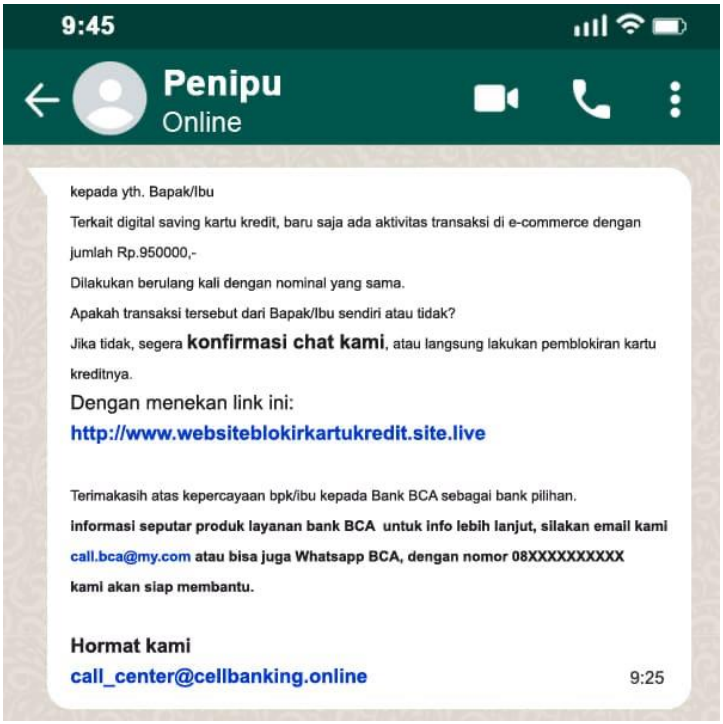
meminta nasabah untuk melakukan transfer dana, yang mana dalam hal ini PT Bank Central Asia Tbk sudah menjelaskan di berbagai akun media sosial resminya bahwa pihak perbankan tidak pernah meminta transfer dana, data pribadi nasabah baik berupa pin atm, 16 digit nomor kartu ATM, dan kode OTP.

Menurut laporan yang diterima dan tercatat oleh sistem, orang tua dengan kisaran usia 40-55 tahun dianggap mudah terjebak berita palsu karena kurangnya pemahaman tentang teknologi yang saat ini berkembang semakin canggih sehingga pelaku kejahatan *online* dapat memanfaatkan psikologi mereka dengan melakukan manipulasi seperti memanfaatkan rasa takut, cemas, panik, atau bahkan memberikan iming-iming atau penawaran hadiah kepada korban. Korban dengan karakter mudah panik selalu menjadi sasaran empuk pelaku untuk semakin memberikan tekanan psikologis yang mendesak korban untuk mengambil keputusan dengan cepat sehingga korban tidak memiliki waktu untuk dapat berpikir dengan jernih dan mencerna apakah berita yang disampaikan adalah berita palsu atau asli.

Kebanyakan pelaku penipuan berita *hoax* yang selama ini beredar di internet memanfaatkan kelemahan paikologis seseorang yaitu rasa keingintahuan yang tinggi akan suatu hal atau berita, tergesa-gesa, dan kelengahan manusia dengan tujuan agar korban tidak menyadari bahwa dirinya adalah sasaran penipuan (Hanik Chumairoh, 2020). Sebagai contoh yang terjadi akhir-akhir ini yaitu penyebaran berita *hoax* terkait naiknya biaya admin transfer antar bank yang disebarluaskan melalui *WhatsApp* dengan mengatasnamakan PT Bank Central Asia Tbk, namun bukan menggunakan nomor resmi BCA yang sudah terverifikasi melainkan nomor pribadi. Modus ini memanfaatkan kepanikan nasabah sebagai momen untuk dapat membobol rekening korban dengan cara mengisi data di *website* yang telah disediakan, nasabah yang panik kemudian membuka *link* tersebut dan melakukan pengisian data-data pribadi yang bersifat sangat rahasia seperti nomor kartu, kode OTP, dsb. Pengisian tersebut dilakukan oleh nasabah tanpa menyadari bahwa berita tersebut adalah palsu dan merupakan modus penipuan *online*.

Tindakan yang diambil pihak bank dalam menyelesaikan kasus penipuan yang dialami oleh nasabah

Melalui *website* resmi PT Bank Central Asia Tbk memberikan informasi terkait dengan ciri-ciri dari modus penipuan yang mengatasnamakan PT Bank Central Asia Tbk sebagai berikut : 1. Mengirimkan *email* atau *Whatsapp* yang menyerupai atau mirip dengan *email* atau pesan *Whatsapp* BCA dengan modus transaksi yang tidak wajar dan mencoba untuk mendapatkan data rahasia nasabah seperti nomor kartu, pin ATM, dan kode OTP, 2. Mengirimkan *file* atau *link* ke nomor pribadi nasabah, jika *link* tersebut dibuka maka akan muncul *website* untuk mengisi data-data nasabah yang bersifat rahasia, 3. Melakukan penipuan melalui telepon seluler dengan modus menyamar sebagai *customer service* bank yang kemudian mengarahkan nasabah untuk melakukan pindah dana ke rekening penipu.



Sementara itu kasus penipuan yang baru-baru ini terjadi adalah dengan menggunakan modus perubahan tarif transfer antar bank menjadi Rp. 150.000/bulan yang mengatas namakan PT Bank Central Asia Tbk. Berita *hoax* ini banyak disebarluaskan melalui *broadcast Whatsapp* yang kemudian menimbulkan kepanikan terhadap nasabah untuk segera menekan tombol *"view"* yang kemudian akan diarahkan ke *website* dimana nasabah diminta untuk mengisi data-data yang bersifat pribadi (Siti Nur Sabrina, 2022). Dalam hal ini Bank BCA menegaskan bahwa pengumuman tersebut adalah tidak benar atau *hoax* dan merupakan aksi dari penipuan. BCA menghimbau agar nasabah lebih berhati-hati dengan cara mengabaikan pesan yang bersifat tidak resmi dan pesan yang menggunakan nomor pribadi (bukan nomor resmi yang sudah terverifikasi), hindari menekan tombol *"view"* dan mengisi data yang bersifat rahasia, segera blokir nomor kontak dan hapus pesan agar tidak terjadi ketidaksengajaan dalam menekan tombol *"view"*.

Executive Vice President (EVP) Corporate Communication and Social Responsibility BCA, Hera F. Haryn menyatakan, "Sebagai perbankan nasional, BCA terus memperkaya wawasan nasabah akan berbagai kejahatan dunia maya yang mengintai. Kami juga terus menyuarakan imbauan kepada masyarakat dan nasabah untuk terus waspada dengan berbagai modus social engineering perbankan. Jika nasabah mendapatkan informasi yang mencurigakan dan mengatasnamakan BCA, nasabah dapat segera menghubungi kantor cabang setempat, atau melalui contact center Halo BCA 1500888 dan aplikasi haloBCA. Jangan pernah bagikan data pribadi perbankan yang bersifat rahasia seperti nomor kartu ATM, PIN, dan OTP."

Apakah hukum di Indonesia tentang tindak pidana *cybercrime* untuk melindungi konsumen/nasabah

Dalam ketentuan yang tertera pada Peraturan Otoritas Jasa Keuangan (POJK) 11/2022 telah ditetapkan bahwa bank memiliki tanggung jawab penuh untuk menjaga ketahanan *cyber* dengan melakukan minimal proses identifikasi aset, perlindungan atas aset, deteksi insiden *cyber*, ancaman, penanggulangan, dan pemulihan inside *cyber* yang telah terjadi. Pada POJK 6/2022 mewajibkan bank yang menggunakan teknologi informasi untuk mengelola data atau informasi nasabah yang bersifat pribadi/rahasia wajib melakukan pengecekan secara berkala terkait dengan kelayakan atau keamanan data nasabah. Apabila kerugian materi yang dialami nasabah adalah kesalahan pihak bank, maka bank wajib bertanggung jawab atas kerugian materi tersebut sebagai mana yang terdapat pada POJK 6/2022 yaitu bank sebagai pelaku usaha yang bergerak dibidang jasa keuangan wajib bertanggung jawab atas kerugian konsumen/nasabah yang timbul akibat kelalaian, kesalahan, atau perbuatan yang bertentangan dengan standar ketentuan peraturan

perundang-undangan yang dilakukan oleh direksi, dewan komisarin, pegawai, atau pihak ketiga yang bekerja untuk kepentingan pribadi, namun apabila kerugian materi disebabkan oleh kelalaian nasabah yang memberikan informasi/data yang bersifat rahasia kepada orang lain maka kerugian tersebut bukan menjadi tanggung jawab bank, melainkan bank berperan sebagai mediator yang membantu mediasi antara korban dengan terduga pelaku.

"Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1 miliar." (Yuffriska Putri Utami, 2021). Dan sebagaimana yang diatur dalam Pasal 31 UU 19/2016 yang berbunyi: "1). Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain. 2). Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. 3). Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang. 4). Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang. Setiap orang yang memenuhi unsur yang dimaksud dalam Pasal 31 ayat (1) atau ayat (2) UU IlE di atas dapat dipidana dengan hukuman penjara paling lama 10 tahun dan/atau denda paling banyak sebesar Rp. 800.000.000.000" (Utin Indah Permata Sari, 2021).

Apakah perbankan sudah memberikan informasi sekaligus mengedukasi nasabah perihal modus penipuan transaksi *online*

Melakukan edukasi dan memberikan informasi kepada nasabah merupakan kewajiban masing-masing perusahaan termasuk dalam bidang perbankan, bank memiliki tanggung jawab untuk memberikan rasa aman kepada nasabah dengan senantiasa melindungi data nasabah sekaligus mengedukasi nasabah terkait produk perbankan serta berita palsu terkait perbankan (Gentur Cahyo, 2022). Berdasarkan *research* yang peneliti lakukan, PT Bank Central Asia Tbk telah memberikan edukasi kepada nasabah terkait berita *hoax* melalui berbagai media salah satu media yang aktif digunakan yaitu *Instagram* dan *website* resmi Bank BCA. Melalui *Instagram* resminya Bank BCA memberikan edukasi berupa konten *reels*, video yang berdurasi satu menit tersebut membahas seputar berita *hoax* yang tersebar di jejaring internet yang mengatasnamakan Bank BCA termasuk memberikan ciri-ciri berita palsu agar nasabah tidak terjebak ke dalam modus penipuan.

Pada akhir tahun lalu tepatnya tanggal 8 Desember 2023, Bank BCA mengajak Indro Warkop untuk berkolaborasi dalam pembuatan konten edukasi dengan slogan "*Don't Know*, Kasih *No*" yang berarti apabila mendapatkan informasi yang tidak jelas

sumbernya maka langkah yang sebaiknya diambil adalah dengan menolak atau "Kasih *No*" serta memblokir nomor atau alamat email tersebut. Tujuan dari dibuatnya konten tersebut adalah untuk memberikan pemahaman tentang berita *hoax* kepada nasabah serta memberikan edukasi terkait langkah-langkah yang seharusnya diambil ketika mendapatkan berita palsu. Selain memberikan edukasi dan informasi melalui media sosial, Bank BCA juga menyebarkan informasi melalui poster yang bisa dilihat oleh nasabah ketika datang langsung ke cabang. Petugas *frontliner* seperti *Teller* dan *Customer Service* juga sering memberikan informasi terkait berita *hoax* serta memberikan edukasi kepada nasabah agar tidak memberikan data-data pribadi seperti PIN, kode OTP (*One-Time Password*), 16 digit nomor kartu, kode CVV (*Card Verification Value*), dan data rahasia lainnya kepada sumber yang tidak jelas untuk menghindari terjadinya kerugian yang dialami oleh nasabah (Lilis Ekayani, 2023).

Tingkat keamanan yang diterapkan oleh bank dalam melindungi data nasabah

Menanggapi keresahan nasabah terkait banyaknya modus penipuan *online* yang dapat merugikan nasabah secara materi, pihak PT Bank Central Asia selalu berupaya untuk meningkatkan keamanan dalam melindungi data nasabah, salah satunya adalah dengan menghadirkan fitur verifikasi wajah pada *Mobile Banking* serta menggunakan sistem otentikasi multi-faktor ketika hendak membuka aplikasi *Mobile Banking* untuk memastikan bahwa yang bertransaksi adalah nasabah yang bersangkutan. Sistem ini mewajibkan penggunanya untuk memasukan kode akses, sidik jari, *face id*, serta PIN yang dapat meningkatkan rasa nyaman dan keamanan nasabah dalam melakukan transaksi secara *online* (Febbyanti Rahmadian dkk, 2020).

Tidak hanya itu, BCA juga senantiasa melakukan *update* data nasabah dengan cara memberikan masa *expired* pada kartu ATM, hal ini bertujuan agar nasabah rajin datang ke cabang untuk mengganti kartu ATM sekaligus melakukan *update* data sehingga pihak bank dapat mengetahui profil nasabah yang terbaru dan memberikan informasi terbaru terkait dengan produk atau layanan perbankan termasuk dengan memberikan edukasi nasabah mengenai modus penipuan yang sering terjadi di perbankan, sehingga diharapkan nasabah dapat lebih berhati-hati ketika mendapatkan berita yang tidak jelas sumbernya.

SIMPULAN

Modus penipuan *online* berupa berita *hoax* yang mengatasnamakan bank merupakan isu yang sampai saat ini menjadi perhatian utama bank untuk dapat menanggulanginya, berbagai upaya telah dilakukan salah satunya dengan tidak henti memberikan edukasi kepada nasabah baik melalui media *online*, iklan, dan pada saat nasabah melakukan transaksi di cabang dengan harapan agar dapat menekan jumlah kasus korban penipuan berita palsu. Tentunya dengan banyaknya berita *hoax* yang tersebar luas di jejaring internet memberikan dampak yang cukup besar terhadap reputasi bank karena bank dianggap lalai dalam kasus ini, padahal hal ini merupakan resiko atau dampak negatif yang ditimbulkan oleh kemajuan teknologi yang terus berkembang. Sebagai bentuk antisipasi bukan hanya pihak bank saja yang mengambil tindakan namun juga nasabah perlu lebih cermat dan teliti lagi dengan berita yang diterima, diharapkan nasabah bisa lebih bijak lagi dalam menerima informasi terlebih apabila sumber informasi yang didapat tidak jelas.

Referensi :

Anak Agung Ayu Astari Fana, Gine Das Prena (2022). Pengaruh *Corporate Social Responsibility*, *Good Corporate Governance*, dan Kepemilikan Manajerial Terhadap Nilai Perusahaan Perbankan Yang Terdaftar Di Bursa Efek Indonesia Periode 2018-2020. Universitas Pendidikan Nasional.

Arsyadona dkk (2020). ISBN: 978-602- 52720-7-3. Manajemen Risiko Reputasi pada Bank Syariah (Dalam Jurnal Seminar Nasional Teknologi Komputer & Sains (SAINTEKS) hal 659).

Budianto, Eka Wahyu Hestya Budianto (2023). Pemetaan Penelitian Risiko Reputasi Pada Perbankan Syariah Dan Konvensional: Studi *Bibliometrik Vosviewer* Dan *Literature Review*. Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Christian Henry Ratulangi, Dr. Anna S. Wahongan, Franky R. Mewengkang (2021). Tindak Pidana *Cybercrime* Dalam Kegiatan Perbankan.

Dalmasius Panggalo (2020). Pengaruh Reputasi Perusahaan Terhadap Keputusan Nasabah Dalam Memilih Produk Pada PT. Bank Sulselbar Cabang Utama Makassar.

Desri Amanda Firdayani Nasution, Ria Septiana, Widya Syaputri, Nurbaiti (2023). Lingkup Dunia *Cyber* di Indonesia

Dewi Chirzah, Rizqy Akbar Ramadhan (2023). *Cyber War:* Ancaman Pada Keamanan Nasional.

Dewi Fatmala Putri, Widya Ratna Sari, Faricha Lita Nabbila (2023). Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan *Digital Banking*.

Febbyanti Rahmadian, Muhammad Maksum, Mara Sutan Rambe. Perlindungan Nasabah Bank Terhadap Tindakan *Phishing*; Studi pada PT Bank Rakyat Indonesia (Persero) Tbk: Jakarta, Indonesia. Universitas Islam Negeri Syarif Hidayatullah.

Firda Laily Mufid, Tioma Roniuli Hariandja. Efektivitas Pasal 28 Ayat (1) UU ITE Tentang Penyebaran Berita Bohong (*Hoax*). Universitas Islam Jember.

Gentur Cahyo Setiono, Irham Rahman (2022). Tanggung Jawab Bank Sebagai Wujud Perlindungan Hukum Bagi Nasabah Kontrak Perbankan.

Hanik Chumairoh (2020). Ancaman Berita Bohong di Tengah Pandemi Covid-19. Program Studi Pemikiran Politik Islam IAIN Kudus.

I Putu Wira Murti, I Wayan Santika. Pengaruh Kepercayaan Nasabah, Bauran Produk dan Bauran

Lokasi Terhadap Transaksi Nasabah.

Lilis Ekayani, Hardianto Djanggih (2023). Perlindungan Hukum Nasabah Terhadap Kejahatan

Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan.

Miftakhur Rokhman Habibi, Isnatul Liviani. Kejahatan Teknologi Informasi (*Cyber Crime*) dan

Penanggulangannya dalam Sistem Hukum Indonesia. UIN Sunan Ampel.

Muhamad Afrizal, Satya Indra Karsa. Strategi *Sales Promotion D'pom Coffee Café* Melalui Media

Sosial *Instagram*. Universitas Islam Bandung.

Muhammad Anthony Aldriano, Mas Agung Priyambodo (2022). *Cyber Crime* Dalam Sudut

Pandang Hukum Pidana.

Muhammad Khairul Faridi (2019). Kejahatan Siber Dalam Bidang Perbankan. Universitas Islam

Indonesia Yogyakarta.

Nunuk Sulisrudatin. Analisa Kasus *Cybercrime* Bidang Perbankan Berupa Modus Pencurian Data

Kartu Kredit. Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma Jakarta.

Nurul Khasanah, Tata Sutabri (2023). Analisis Kejhatan *Cybercrime* Pada Peretasan

dan Penyadapan Aplikasi *Whatsapp*.

Rian Dwi Hapsari, Kuncoro Galih Pambayun (2023). Ancaman *Cyber Crime* di Indonesia; Sebuah

Tinjauan Pustaka Sistematis. Institut Pemerintahan Dalam Negeri.

Sastrawan Manullang dkk. ISBN : 978-602-440-204-4. Teori dan Teknik Analisis *Stakeholder*.

Siti Nur Shabrina, Zamzani, Teguh Setiawan. Analisis Teks Hoaks Seputar Informasi Bank; Kajian

Bahasa Perspektif Analisis Wacana Kritis dan Linguistik Forensik. Universitas Negeri Yogyakarta.

Syeren Al Gista, Dewi Prastiwi. Vol. 6, no 3, (2022). Pengaruh *Corporate Social Responsibility*