**ISLAMIC BANKING AND FINANCE JOURNAL 5 (1)**
**JURNAL PERBANKAN DAN KEUANGAN SYARIAH**
P-ISSN: 2828-4402 E-ISSN: 2963-9034

# KEBIJAKAN PENANGANAN *CYBER CRIME* PENGGUNA *M-BANKING* DALAM PENILAIAN LOYALITAS NASABAH BSI KC. SINJAI

**Andi Jaatsiyah Fath Falaq Am. Nur[1], Andi Patimbangi[2]**

[12]Institut Agama Islam Negeri Bone

ajaatsiyahaat@gmail.com[1] andipatimbangi@yahoo.com[2]

**ABSTRACT**

*The purpose of this study is (1) To find out how the policies implemented by BSI KC. Sinjai in handling cyber crime on mobile banking users, (2) To find out how customer behavior responds to BSI Branch Sinjai's policies in handling cyber crime on mobile banking users. The type of research used is field research using a qualitative approach. The data collection techniques used are interviews and documentation. The analysis techniques used are data decomposition, data presentation and drawing conclusions. The results of this study are (1) The policies implemented by BSI Sinjai Regency show alignment with Philipus M. Hadjon's legal protection theory, which emphasizes preventive and repressive government actions. The policies adopted by BSI Sinjai Regency show alignment with Law Number 8 of 1999 concerning Consumer Protection and Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), (2) BSI Sinjai Branch has significant implications for maintaining customer loyalty. Philip Kotler, identified four main dimensions of loyalty, namely repeat intention, word-of-mouth, price sensitivity, and complaining behavior. BSI's policy in handling cyber crime directly affects these four dimensions.*
***Keywords:*** *Cyber Crime; Loyalty; Mobile Banking; Policy*

**ABSTRAK**

Tujuan penelitian ini adalah (1) Untuk mengetahui bagaimana kebijakan yang dilakukan oleh pihak BSI KC. Sinjai dalam penanganan cyber crime pada pengguna mobile banking, (2) Untuk mengetahui bagaimana perilaku nasabah menanggapi kebijakan pihak BSI Cabang Sinjai dalam penanganan cyber crime pada pengguna mobile banking. Jenis penelitian yang digunakan adalah penelitian lapangan *(field research)* dengan menggunakan pendekatan kualitatif. Teknik pengumpulan data yang digunakan adalah wawancara dan dokumentasi. Teknik analisis yang digunakan adalah dekomposisi data, penyajian data dan penarikan kesimpulan. Hasil penelitian ini adalah (1) Kebijakan yang dilakukan BSI Kabupaten Sinjai menunjukkan keselarasan dengan teori perlindungan hukum Philipus M. Hadjon, yang menekankan pada tindakan preventif dan represif pemerintah. Kebijakan yang diambil oleh BSI Kabupaten Sinjai menunjukkan keselarasan dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), (2) BSI Cabang Sinjai memiliki implikasi signifikan terhadap pemeliharaan loyalitas nasabah. Philip Kotler, mengidentifikasi empat dimensi utama loyalitas, yaitu *repeat intention* (niat untuk menggunakan kembali), *word-of-mouth* (dari mulut ke mulut), *price sensitivity* (sensitivitas terhadap harga), dan *complaining behavior* (perilaku dalam menyampaikan keluhan). Kebijakan BSI dalam menangani *cyber crime* secara langsung memengaruhi keempat dimensi ini.

**Kata Kunci**: *Cyber Crime;* Kebijakan*;* Loyalitas; *Mobile Banking*

## I. PENDAHULUAN

Di era digital yang semakin maju, nasabah dapat melakukan transaksi keuangan dengan lebih mudah dan nyaman saat menggunakan *mobile banking*, namun

P-ISSN: 2828-4402 E-ISSN: 2963-9034

terdapat ancaman terhadap keamanan data dan informasi mereka. Pada tahun 2020, terdapat 88.414.296 serangan *cyber* di Indonesia. Dengan 29.188.645 serangan, Februari menjadi bulan dengan jumlah serangan tertinggi. Menurut riset Annur dalam penelitian yang dilakukan oleh Hidayatputra tahun 2023, Indonesia menduduki peringkat ketiga kasus kebocoran data pada kuartal ketiga tahun 2022, setelah Prancis dan Rusia. Gugatan hukum atas kebocoran data tersebut melibatkan 12,74 juta akun (Hidayatputra Pratama & Nurhayati, 2023). Kejahatan siber yang lebih serius dapat muncul di masa mendatang akibat kasus kebocoran ini. Sejak awal tahun 2022 hingga saat ini, Badan Siber dan Sandi Negara (BSSN) melaporkan telah terjadi 976.429.996 serangan siber pada tahun 2022 atau hampir setara dengan satu miliar serangan siber. Dibandingkan tahun sebelumnya, serangan ini tentu telah meningkat beberapa kali lipat (Hidayatputra Pratama & Nurhayati, 2023).

Penilitian yang dilakukan Barquin pada tahun 2019 dalam riset Mckinsey & Company menyatakan bahwa Indonesia merupakan negara di Asia yang mengadopsi perbankan digital tercepat dikarenakan banyaknya pengguna internet di Indonesia. Banyaknya jumlah pengguna internet tentu berakibat pada jumlah pengguna *e-banking* di Indonesia dimana kenaikan yang dialami lebih dari 20% pengguna pada hampir di setiap bank yang ada di Indonesia (Barquin, Gantes, HV, & Shrikhande, 2019). penggunaan internet dan aplikasi digital perbankan yang semakin bertambah tentunya juga akan memunculkan dampak negatif berupa ancaman keamanan digital atau yang biasa disebut dengan istilah *cyber crime* (Bahl, 2012).

Pembahasan mengenai *cyber crime* pada layanan perbankan sudah banyak dibahas oleh peneliti sebelumnya, diantaranya penelitian (Purwani, 2023) yang lebih berfokus dalam membahas sebuah kasus hipotetis serangan *spearphishing* yang melibatkan pelaku, korban, beserta pihak-pihak lain yang tanpa disadari juga terlibat dalam kejahatan siber selain itu ada juga penelitian (Utin Indah Permata Sari, 2022) Hasil penelitian menunjukkan bahwa pengaturan hukum pidana terkait tindak pidana siber di Indonesia belum sepenuhnya memadai. Meskipun Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur beberapa aspek, namun masih diperlukan harmonisasi dan penyesuaian lebih lanjut seiring dengan perkembangan tindak pidana siber

P-ISSN: 2828-4402 E-ISSN: 2963-9034

Berdasarkan penelitian yang telah diuraikan sebelumnya, secara spesifik pembahasan mengenai kebijakan *cyber crime* pada pengguna mobile banking terkhusus dalam menilai loyalitas nasabah belum pernah dilakukan sebelumnya, untuk itu penelitian ini hadir guna membahas fenomena tersebut. Sehingga hal ini yang menjadi perbedaan dan sekaligus kebaharuan dari penelitian-penelitian sebelumnya dengan penelitian yang akan dilakukan nantinya.

Penelitian mengenai kebijakan penanganan *cyber crime* pada pengguna *mobile banking* dalam menilai loyalitas nasabah memiliki urgensi yang sangat penting dalam dunia perbankan digital sekarang ini. Dengan semakin berkembangnya teknologi dan penggunaan layanan perbankan melalui *platform mobile*, keamanan dan kepercayaan nasabah menjadi prioritas utama bagi bank. Ancaman *cyber crime* seperti pencurian identitas, penipuan online, dan serangan malware dapat merugikan nasabah dan merusak reputasi bank. Dalam konteks ini, penelitian yang mendalam mengenai kebijakan penanganan *cyber crime* menjadi krusial untuk melindungi data pribadi nasabah, mencegah aksi kriminal yang merugikan, dan meningkatkan keamanan transaksi finansial. Dengan adanya perlindungan yang kuat akan membangun kepercayaan nasabah, menjaga loyalitas mereka, dan mempertahankan reputasi bank.

Berdasarkan penjelasan tersebut, maka penelitian ini bertujuan (1) Untuk mengetahui bagaimana kebijakan yang dilakukan oleh pihak BSI Cabang Sinjai dalam penanganan cyber crime pada pengguna mobile banking, (2) Untuk mengetahui bagaimana perilaku nasabah menanggapi kebijakan pihak BSI Cabang Sinjai dalam penanganan cyber crime pada pengguna mobile banking.

## II. TINJAUAN PUSTAKA

### Mobile Banking

*Mobile banking* pada perbankan dapat menawarkan layanan seluler sebagai untuk memfasilitasi transaksi daring bagi nasabahnya. Dengan kata lain, ini adalah metode menggunakan telepon pintar atau perangkat seluler lainnya untuk melakukan transaksi perbankan. Jika memiliki koneksi internet yang andal, maka dapat menggunakan layanan ini kapan saja dan dari lokasi mana pun. Perbankan seluler adalah jenis layanan atau fasilitas perbankan yang memanfaatkan perangkat komunikasi portabel, seperti telepon pintar, dan menawarkan kemampuan transaksi perbankan melalui aplikasi seluler. Melalui penggunaan telepon seluler dan layanan perbankan seluler, nasabah dapat menghemat lebih banyak waktu dan tenaga dengan

P-ISSN: 2828-4402 E-ISSN: 2963-9034

menyelesaikan transaksi perbankan yang sebelumnya diselesaikan secara manual, seperti langsung mendatangi bank untuk menyelesaikan transaksi (Miftahuddin & Hendarsyah, 2019).

*Mobile banking* adalah salah satu layanan keuangan yang diciptakan dengan teknologi GPRS *(General Package Radio Service).* GPRS merupakan teknologi yang menyalurkan data melalui perangkat seluler dan dapat disalurkan dalam bentuk aplikasi atau pesan. Manfaat layanan *mobile banking*, khususnya kemudahan penggunaannya, ditentukan oleh persepsi nasabah bank terhadap kapasitas mereka dalam memanfaatkan *mobile banking*, yang diukur dengan metrik seperti efisiensi transaksi, efisiensi waktu, kemudahan operasional, dan fleksibilitas. Oleh karena itu, dapat dikatakan bahwa semakin banyak masyarakat yang meyakini bahwa layanan tersebut mudah digunakan, maka semakin besar pula manfaat yang akan diperoleh (Sari, Fasa, & Suharto, 2021).

Kelemahan dari *mobile banking* ialah ketergantungan terhadap ketersediaan jaringan seluler operator yang bersangkutan. Jika terjadi *blankspot* atau ketersediaan jaringan, maka layanan *mobile banking* tidak bisa dilakukan. Hal tersebut sebenarnya bukanlah tanggung jawab bank melainkan tanggung jawab penyedia operator seluler dan internet provider yang digunakan oleh nasabah untuk mengakses layanan *mobile banking*. Namun demikian hal tersebut dapat mengganggu transaksi nasabah terutama jika nasabah dalam kondisi *urgent* (Mainata, 2018).

### *Cyber Crime*

Tindak pidana di dunia maya yang menggunakan jaringan komputer sebagai alat dan jaringan internet sebagai medianya disebut dengan istilah kejahatan dunia maya. Semua kegiatan melawan hukum yang dilakukan melalui sistem jaringan komputer dan internet dengan tujuan untuk mendapatkan keuntungan dengan cara merugikan orang lain secara kolektif disebut dengan kejahatan dunia maya. Dan dalam pengertian sempit, kejahatan dunia maya mengacu pada setiap kegiatan melawan hukum yang bertujuan untuk membahayakan sistem keamanan komputer dan data yang diproses oleh sistem komputer. (Syahputra, 2020).

Terdapat beberapa jenis cyber crime yang umumnya sering terjadi sebagaimana yang dikutip dari berbagai sumber tepercaya, antara lain sebagai berikut (Syahputra, 2020) :

P-ISSN: 2828-4402 E-ISSN: 2963-9034

*1) Unauthorized Aces*

Kejahatan yang terjadi ketika seseorang secara ilegal mengakses atau menyusup ke dalam skema jaringan komputer tanpa izin atau sepengetahuan pemiliknya.

*2) Illegal Contents*

Pelanggaran yang melibatkan pengunggahan informasi ke internet yang tidak akurat, tidak sopan, dan dapat dianggap sebagai pelanggaran hukum atau gangguan ketertiban umum.

3) Penyebaran Virus Secara Sengaja

Biasanya, email digunakan untuk menyebarkan virus. Orang-orang yang memiliki sistem email yang terinfeksi virus sering kali tidak menyadari hal ini. Email mereka kemudian digunakan untuk menyebarkan infeksi ini ke lokasi lain.

*4) Cyber Espionage, Sabotage dan Extortion*

*Cyber Espionage* adalah kejahatan yang melibatkan pembobolan sistem jaringan komputer pihak target dan menggunakan internet untuk melakukan kegiatan memata-matai mereka. Kejahatan seperti pemerasan dan sabotase melibatkan gangguan, kerusakan, atau penghancuran data, program komputer, atau sistem jaringan komputer yang terhubung ke internet.

*5) Carding*

Pencurian nomor kartu kredit dari pengguna layanan perbankan atau organisasi sejenis lainnya dan penggunaannya dalam transaksi daring dikenal sebagai *carding.*

*6) Hacking dan Cracker*

Istilah *hacker* secara umum, menggambarkan seseorang yang sangat tertarik untuk memeriksa sistem komputer secara menyeluruh dan mempelajari cara meningkatkan kemampuannya. Aktivitas cracking daring dapat dilakukan dalam berbagai bentuk, termasuk mengambil alih akun orang lain, mengambil alih situs web, menyelidiki, menyebarkan malware, atau melumpuhkan korban. DoS *(Denial Of Service)* adalah tindakan terakhir. Tujuan dari serangan *denial-of-service* (DoS) adalah membuat target tidak dapat beroperasi dengan menyebabkannya hang atau crash layanan.

P-ISSN: 2828-4402 E-ISSN: 2963-9034

*7) Cybersquatting And Typosquatting*

*Cybersquatting* merupakan indakan mendaftarkan nama domain perusahaan orang lain dan kemudian mencoba menjualnya ke perusahaan itu dengan harga lebih tinggi. *Typosquatting,* atau membuat domain palsu yang tampak seperti nama domain orang lain, adalah tindakan illegal lainnya.

*8) Cyber Terorism*

Serangan terhadap data, program komputer, sistem, dan informasi yang menimbulkan ancaman bagi pemerintah atau penduduknya, seperti membobol situs web militer atau pemerintah, merupakan contoh kegiatan yang disengaja dan bermotif politik.

## Perlindungan Hukum bagi Nasabah dari Kejahatan Menggunakan Teknologi Informasi (Cyber Crime).

Pembahasan mengenai perlindungan hukum bagi nasabah maupun bank dari *cyber crime* yang berkaitan dengan UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, kita akan melihat dari beberapa teori mengenai perlindungan hukum. Menurut pendapat Philipus M. Hadjon menjelaskan bahwa perlindungan hukum bagi rakyat sebagai tindakan pemerintah yang bersifat preventif dan represif (Ni Nyoman Anita Candrawati, 2014). Perlindungan hukum yang preventif bertujuan untuk mencegah terjadinya sengketa yang mengarahkan tindakan pemerintah bersikap hati-hati dalam pengambilan keputusan berdasarkan diskresi, dan perlindungan yang represif bertujuan untuk menyelesaikan terjadinya sengketa termasuk penanganannya di lembaga peradilan.

Teori perlindungan konsumen selanjutnya adalah *due care theory* gagasan tentang perlindungan konsumen. Filosofi ini menegaskan bahwa pelaku korporasi memiliki tanggung jawab untuk berhati-hati saat memasarkan barang dan jasa mereka. Mereka tidak dapat dimintai pertanggungjawaban selama mereka menangani barang dagangan mereka dengan hati-hati. Pelanggan harus dapat menunjukkan bahwa pelaku korporasi melanggar prinsip kehati-hatian agar mereka dapat dimintai pertanggungjawaban. Dalam hal ini, konsumen adalah pihak aktif yang menunjukkan kesalahan pelaku usaha, sedangkan pelaku usaha adalah pihak pasif (See, 2022).

P-ISSN: 2828-4402 E-ISSN: 2963-9034

## Loyalitas

Menurut (Adila, 2017) loyalitas pelanggan adalah kualitas konsumen yang secara konsisten menepati janjinya untuk menggunakan barang atau jasa yang sama, meskipun perilaku tersebut dilakukan tanpa mempertimbangkan barang atau jasa tersebut. Dengan demikian, dapat dikatakan bahwa keseimbangan dan kombinasi antara kepuasan dan keluhan pelanggan menghasilkan loyalitas terhadap suatu merek atau jasa tertentu. Pelanggan yang loyal adalah pelanggan yang merasa puas terhadap suatu produk atau jasa tertentu.

Menurut Kotler yang dikutip oleh Gita Oktaviani (2019), konsep loyalitas pelanggan diukur dengan empat indikator yang menggambarkan sikap positif dan perilaku pembelian ulang yaitu (Oktaviani, 2019) :

1. *Purchase Intention*

   Indikator pertama loyalitas Rasa minat beli pelanggan, atau keinginan kuat mereka untuk melakukan pembelian atau transaksi ulang barang atau jasa di bisnis yang sama di masa mendatang. Keinginan kuat untuk membeli kembali barang atau jasa dari bisnis yang sama sebenarnya merupakan tanda perilaku konsumen yang loyal.

2. *Word-of-mouth*

   Perpindahan informasi dari mulut ke mulut, diukur sebagai indikasi kedua. Dari mulut ke mulut yang dimaksud adalah ketika klien memuji bisnis dan merekomendasikannya kepada orang lain. Jika pelanggan siap merekomendasikan dan memberi tahu orang lain, maka dapat dianggap mereka loyal. Loyalitas pelanggan meningkat ketika lebih banyak orang menyebarkan berita tentang aspek positif perusahaan dan mempromosikannya kepada orang lain.

3. *Price Sensivity*

   Indikator ketiga adalah pengukuran loyalitas pelanggan, atau kesan pelanggan terhadap kepekaan harga. Tujuan kepekaan harga adalah untuk memastikan bahwa konsumen tidak menolak tawaran produk dari bisnis pesaing atau terpengaruh oleh tawaran harga yang lebih rendah dari bisnis pesaing. Tawaran dari pesaing dapat berupa hadiah, diskon, suku bunga tinggi, atau insentif lainnya.

4. *Complaining Behavior*

   Indikator terakhir adalah Pengukuran loyalitas klien, atau bagaimana konsumen memandang keluhan. Pelanggan yang berperilaku seperti ini tidak ragu

P-ISSN: 2828-4402 E-ISSN: 2963-9034

untuk menyampaikan keluhan mereka kepada perusahaan di masa mendatang karena mereka telah mengembangkan hubungan yang.

## III.METODE PENELITIAN

Penelitian yang akan dilakukan ini merupakan penelitian *field research* (penelitian lapangan). Penelitian lapangan *(field research),* yaitu suatu penelitian yang dilakukan di lapangan atau di lokasi penelitian. Metode penelitian ini berfokus pada pengumpulan data dan informasi yang akan dilakukan secara langsung di lokasi penelitian, di mana peneliti memilih tempat di Bank Syariah Indonesia (BSI) Kabupaten SInjai. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan kualitatif deskriptif. Teknik pengumpulan data yang digunakan adalah wawancara dan dokumentasi. Teknik analisis yang digunakan pada penelitian ini adalah dekomposisi data, penyajian data dan penarikan kesimpulan.

## IV.HASIL DAN PEMBAHASAN

### HASIL PENELITIAN

### Kebijakan yang Dilakukan Oleh Pihak BSI Cabang Sinjai dalam Penanganan Cyber Crime Pada Pengguna mobile banking

Sebagai salah satu solusi dalam mengatasi hal ini, diperlukan upaya preventif yang komprehensif, upaya pencegahan harus selalu menjadi aspek fokus dari sistem perbankan. Berdasarkan wawancara yang dilakukan dengan Bapak Muh. Lutfi Ermus selaku narasumber 1 PSO di BSI Kabupaten Sinjai. Berikut penuturannya :

> "Keamanan transaksi *mobile banking* menjadi tanggung jawab utama bagi kami selaku pelaksana kebijakan di perbankan. Kami sangat memahami bahwa dunia digital saat ini sangat rentan terhadap ancaman *cyber crime*, olehnya kami dari pihak bank tentu akan melakukan upaya pencegahan secara maksimal. Salah satu langkah penting yang dilakukan penentu kebijakan di BSI adalah dengan meningkatkan keamanan sistem *mobile banking*. BSI telah meninggalkan aplikasi BSI *Mobile* dan berganti menggunakan aplikasi *mobile banking* yang terbaru yakni Byond dengan otentikasi multi-faktor sebagai lapisan keamanan tambahan." (Ermus, 2024).

Hal serupa juga di ungkapkan oleh Ibu Fadillah Sulistiani H selaku narasumber 2 *pawning appraisal* di BSI Kabupaten sinjai. Berikut penuturannya :

> "Untuk memastikan keamanan transaksi mobile banking, pihak bank menerapkan berbagai tindakan pencegahan untuk melindungi keamanan data nasabah, diantaranya dengan meningkatkan sistem keamanan dalam penggunaan *mobile banking* dengan menggunakan verifikasi dua langkah, dimana nasabah tidak hanya melakukan aktivasi menggunakan nomor telepon

P-ISSN: 2828-4402 E-ISSN: 2963-9034

> saja tetapi juga dengan menggunakan email yang aktif sehingga kode verifikasinya tidak hanya masuk melalui SMS saja melainkan juga masuk melalui email sehingga sulit untuk diakses oleh orang yang tidak bersangkutan." (Sulistiani, 2024).

Kebijakan represif hadir sebagai salah satu pilar penting dalam menanggulangi ancaman ini. Kehadiran kebijakan represif yang kuat mencerminkan keseriusan suatu negara dan lembaga keuangan dalam menangani *cyber crime*. Berdasarkan wawancara yang dilakukan dengan Bapak Muh. Lutfi Ermus selaku narasumber 1 PSO di BSI Kabupaten Sinjai. Berikut penuturannya :

> "Meskipun di BSI Kabupaten Sinjai tidak memiliki tim siber, tapi kami selalu bersinergi dan berkolaborasi dalam menangani ancaman *cyber crime*. Perlu diketahui sebelumnya bahwa pada perbankan khususnya di BSI penentu kebijakan adalah pusat dimana kami hanya pelaksana kebijakan, jadi yang bertanggung jawab terhadap penyelidikan kasus *cyber crime* adalah pusat. Namun, hal itu bukan berarti membuat kami mengabaikan ancaman *cyber crime* yang terjadi pada nasabah, itulah sebabnya kami melakukan berbagai upaya di antaranya adalah menambah jam kerja pada hari libur untuk memfasilitasi nasabah yang mengalami gangguan pada aplikasi *mobilenya*. Selain itu, pernah terjadi gangguan besar-besaran pada sistem BSI sehingga mengganggu operasional bank, adapun kebijakan yang dikeluarkan pihak BSI pusat adalah dengan mengganti seluru server dan perangkat kami dengan yang lebih terbaru dan memadai." (Ermus, 2024).

Hal serupa juga di ungkapkan oleh Ibu Fadillah Sulistiani H selaku narasumber 2 *pawning appraisal* di BSI Kabupaten sinjai. Berikut penuturannya :

> "Di BSI pernah terjadi gangguan sistem yang mengakibatkan terhambatnya operasional kantor, tapi hal itu tidak berlangsung lama karena kerja cepat tanggap oleh pihak-pihak keamanan di pusat. Selain itu, kami di BSI Kabupaten Sinjai diarahkan untuk mengganti server kami. Sebagai upaya dalam mengatasi gangguan lainnya pada pengguna *mobile banking* agar tidak terjadi kasus serupa kedua kalinya maka kami meluncurkan layanan *weekend banking*. *Weekend banking* adalah layanan yang kami sediakan dimana nasabah diperbolehkan ke kantor ketika mengalami gangguan atau gagal sistem pada aplikasi mobilenya." (Sulistiani, 2024).

Bank memiliki protokol komunikasi internal yang mengatur bagaimana informasi tentang insiden keamanan siber harus disampaikan kepada pihak-pihak terkait di internal bank. Berdasarkan wawancara yang dilakukan dengan Bapak Muh. Lutfi Ermus selaku narasumber 1 PSO di BSI Kabupaten Sinjai. Berikut penuturannya :

> "Dalam menghadapi ancaman *cyber crime* yang semakin kompleks dan canggih, pihak bank mengambil langkah-langkah proaktif dan komprehensif untuk melindungi keamanan data nasabah. Bank memiliki protokol komunikasi internal yang jelas dan terstruktur. Protokol ini mengatur bagaimana informasi terkait insiden keamanan siber harus disampaikan kepada pihak-pihak terkait di internal bank, termasuk manajemen senior, dewan direksi, dan unit-unit

terkait lainnya. Tujuannya adalah untuk memastikan bahwa informasi yang akurat dan relevan sampai kepada pihak yang tepat, sehingga mereka dapat mengambil tindakan yang diperlukan." (Ermus, 2024).

Hal serupa juga di ungkapkan oleh Ibu Fadillah Sulistiani H selaku narasumber 2 *pawning appraisal* di BSI Kabupaten sinjai. Berikut penuturannya :

> "Bank memiliki protokol komunikasi internal yang mengatur alur informasi terkait insiden keamanan siber. Protokol ini memastikan bahwa informasi akurat dan relevan tersampaikan kepada pihak-pihak terkait di internal bank, termasuk manajemen senior, dewan direksi, dan unit-unit terkait lainnya. Ketika ancaman siber terdeteksi, tim respons insiden akan segera melakukan identifikasi untuk mengetahui jenis serangan, sumbernya, dan dampaknya. Setelah ancaman teridentifikasi, tim akan mengisolasi sistem atau jaringan yang terinfeksi untuk mencegah penyebaran lebih lanjut." (Sulistiani, 2024).

### Loyalitas nasabah menanggapi kebijakan pihak BSI Cabang Sinjai dalam penanganan cyber crime pada pengguna mobile banking

Berdasarkan wawancara yang dilakukan dengan Ibu Devi Sriana selaku narasumber 3 Costumer Service di BSI Kabupaten Sinjai. Berikut penuturannya :

> "Kebijakan penanganan cyber crime yang efektif dapat meningkatkan kepercayaan dan keamanan nasabah dalam menggunakan layanan mobile banking. Hal tersebut dapat dilihat dari meningkatnya penggunaan aplikasi mobile banking yang baru yaitu byond di kalangan nasabah karena fiturnya lebih mudah dan aman. Selanjutnya, nasabah akan merasa nyaman dan aman menggunakan layanan *mobile banking* jika mereka percaya bahwa bank memiliki kebijakan yang kuat dalam menangani *cyber crime*. Kami melihat walaupun tidak selalu namun terkadang nasabah merekomendasikan teman yang diajaknya untuk menggunakan aplikasi byond. Selain Itu, saya melihat bahwa ketika nasabah terbiasa menggunakan satu layanan *mobile banking* maka ia tidak akan mudah beralih walaupun dengan penawaran harga yang lebih murah. Hal tersebut dikarenakan kami selalu memprioritaskan kenyamanan nasabah dalam menggunakan aplikasi byond. Menurut saya pribadi, nasabah sepertinya sudah tidak canggung lagi ketika mengalami masalah dalam penggunaan byond. Pengalaman pernah kami mendapat banyak keluhan, sebagai bentuk penanganan kami yaitu dengan membuka layanan *weekend banking* agar kami dapat memberi solusi secara cepat dan menyuluruh." (Devi Sriana, 2024).

## PEMBAHASAN HASIL PENELITIAN

### Kebijakan yang Dilakukan Oleh Pihak BSI Cabang Sinjai dalam Penanganan Cyber Crime Pada Pengguna mobile banking

BSI Kabupaten Sinjai memiliki komitmen kuat dalam menjaga keamanan informasi dan melindungi nasabah dari ancaman *cyber crime*. Kebijakan penanganan *cyber crime* mereka mencakup berbagai aspek, mulai dari pencegahan hingga

penindakan. Dalam hal pencegahan, BSI secara aktif memberikan edukasi kepada nasabah mengenai potensi risiko kejahatan siber dan cara menghindarinya. Sosialisasi dilakukan melalui berbagai saluran, seperti situs web resmi, media sosial, dan seminar.

Kebijakan yang dilakukan oleh BSI Kabupaten Sinjai menunjukkan keselarasan dengan teori perlindungan hukum Philipus M. Hadjon, yang menekankan pada tindakan preventif dan represif pemerintah. Penerbitan aplikasi *mobile banking* Byond yang lebih aman merupakan langkah preventif BSI dalam mencegah potensi kejahatan siber. Aplikasi ini dirancang dengan fitur keamanan yang lebih canggih, meminimalisir risiko pembobolan dan penyalahgunaan data nasabah. Di sisi lain, tindakan BSI mengganti server dan menambah jam kerja operasional untuk menangani keluhan nasabah terkait *mobile banking* adalah langkah represif. Penggantian server bertujuan untuk meningkatkan performa dan keamanan sistem, mengatasi masalah teknis yang mungkin terjadi. Penambahan jam kerja operasional menunjukkan respons cepat BSI terhadap keluhan nasabah, memastikan setiap masalah terkait *mobile banking* dapat segera tertangani.

Kebijakan yang diambil oleh BSI Kabupaten Sinjai menunjukkan keselarasan dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Berdasarkan UU perlindungan konsumen pasal 4 huruf c yaitu BSI memberikan informasi yang jelas dan benar mengenai layanan *mobile banking* Byond, termasuk fitur keamanan yang ditawarkan. Pasal 7 huruf b yaitu BSI menjamin keamanan dan kenyamanan konsumen dalam menggunakan layanan *mobile banking* dengan terus meningkatkan sistem keamanan dan menangani keluhan nasabah dengan cepat. Pasal 19 BSI bertanggung jawab atas kerugian yang diderita konsumen akibat penggunaan layanan *mobile banking*, kecuali jika kerugian tersebut disebabkan oleh kesalahan konsumen sendiri.

## Loyalitas nasabah menanggapi kebijakan pihak BSI Cabang Sinjai dalam penanganan cyber crime pada pengguna mobile banking

Bank Syariah Indonesia (BSI) di Kabupaten Sinjai, sebagai bagian dari entitas nasional, memprioritaskan keamanan *cyber* secara ketat, terutama dalam layanan *mobile banking* melalui aplikasi BSI *Mobile* (Byond). Kebijakan keamanan BSI dibangun di atas fondasi teknologi enkripsi SSL yang kuat, memastikan kerahasiaan data nasabah selama transmisi. Autentikasi berlapis, termasuk penggunaan biometrik dan 2FA,

P-ISSN: 2828-4402 E-ISSN: 2963-9034

memperkuat perlindungan akun dari akses ilegal. Sistem pemantauan aktivitas mencurigakan secara real-time dan respons insiden yang cepat menjadi kunci dalam mendeteksi dan mengatasi ancaman *cyber crime*.

Loyalitas nasabah, sebagai konstruk multidimensional mencerminkan preferensi dan komitmen berkelanjutan pada individu terhadap suatu entitas, dalam konteks ini yang dimakasud adalah BSI Cabang Sinjai. Dalam ranah *mobile banking*, loyalitas menjadi krusial mengingat tingginya risiko *cyber crime* yang dapat menggerus kepercayaan nasabah. Kebijakan penanganan *cyber crime* yang diterapkan oleh BSI Cabang Sinjai memiliki implikasi signifikan terhadap pembentukan dan pemeliharaan loyalitas nasabah. Philip Kotler, pakar pemasaran terkemuka, mengidentifikasi empat dimensi utama loyalitas, yaitu *repeat intention* (niat untuk menggunakan kembali), *word-of-mouth* (dari mulut ke mulut), *price sensitivity* (sensitivitas terhadap harga), dan *complaining behavior* (perilaku dalam menyampaikan keluhan). Kebijakan BSI dalam menangani *cyber crime* secara langsung maupun tidak langsung memengaruhi keempat dimensi ini.

Kebijakan BSI yang responsif dan efektif dalam menangani *cyber crime* berpotensi memperkuat loyalitas nasabah melalui beberapa cara. Pertama, nasabah yang merasa aman dan terlindungi saat menggunakan *mobile banking* BSI cenderung memiliki niat yang kuat untuk terus menggunakan layanan tersebut (*repeat intention*). Pengalaman positif dalam penanganan *cyber crime* meningkatkan kepercayaan nasabah terhadap BSI. Kedua, nasabah yang puas dengan penanganan *cyber crime* oleh BSI cenderung akan menceritakan pengalaman positif mereka kepada orang lain (*word-of-mouth*). Efek *word-of-mouth* ini dapat menyebar luas dan menarik nasabah baru. Reputasi BSI sebagai lembaga yang peduli terhadap keamanan nasabah akan semakin meningkat. Ketiga, ketika nasabah merasa aman dan nyaman dengan layanan *mobile banking* BSI, sensitivitas mereka terhadap harga atau biaya layanan cenderung menurun (*price sensitivity*). Mereka lebih fokus pada nilai dan manfaat yang diberikan oleh BSI, bukan hanya pada harga. Keempat, nasabah yang loyal cenderung lebih aktif dalam menyampaikan keluhan mereka kepada BSI jika mengalami masalah atau ketidakpuasan (*complaining behavior*). Mereka percaya bahwa BSI akan mendengarkan dan menanggapi keluhan mereka dengan baik. Perilaku *complaining* yang konstruktif ini memberikan kesempatan bagi BSI untuk memperbaiki diri dan meningkatkan kualitas layanan.

P-ISSN: 2828-4402 E-ISSN: 2963-9034

Secara keseluruhan, kebijakan BSI Cabang Sinjai dalam penanganan *cyber crime* memiliki peran krusial dalam membentuk dan memelihara loyalitas nasabah. Dengan memberikan perlindungan yang efektif dan responsif, BSI tidak hanya meminimalkan risiko *cyber crime*, tetapi juga membangun kepercayaan dan memperkuat komitmen nasabah terhadap layanan *mobile banking* mereka. Hal ini sejalan dengan teori Kotler, di mana keempat dimensi loyalitas saling terkait dan dipengaruhi oleh pengalaman nasabah dengan kebijakan dan layanan yang ditawarkan oleh lembaga keuangan.

## V. KESIMPULAN DAN SARAN

### Kesimpulan

Berdasarkan uraian penjelasan pada pembahasan tersebut, dapat disimpulkan bahwa BSI Kabupaten Sinjai memiliki komitmen kuat dalam menjaga keamanan informasi dan melindungi nasabah dari ancaman *cyber crime*. Kebijakan yang dilakukan oleh BSI Kabupaten Sinjai menunjukkan keselarasan dengan teori perlindungan hukum Philipus M. Hadjon, yang menekankan pada tindakan preventif dan represif pemerintah. Penerbitan aplikasi *mobile banking* Byond yang lebih aman merupakan langkah preventif BSI dalam mencegah potensi *cyber crime*. Di sisi lain, tindakan BSI mengganti server dan menambah jam kerja operasional untuk menangani keluhan nasabah terkait *mobile banking* adalah langkah represif. Penggantian server bertujuan untuk meningkatkan performa dan keamanan sistem, mengatasi masalah teknis yang mungkin terjadi. Di sisi lain, tindakan BSI mengganti server dan menambah jam kerja operasional untuk menangani keluhan nasabah terkait *mobile banking* adalah langkah represif. Penggantian server bertujuan untuk meningkatkan performa dan keamanan sistem, mengatasi masalah teknis yang mungkin terjadi. Penambahan jam kerja operasional menunjukkan respons cepat BSI terhadap keluhan nasabah, memastikan setiap masalah terkait *mobile banking* dapat segera tertangani. Kebijakan yang diambil oleh BSI Kabupaten Sinjai menunjukkan keselarasan dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

BSI Kabupaten SInjai tidak hanya meminimalkan risiko *cyber crime*, tetapi juga membangun kepercayaan dan memperkuat komitmen nasabah terhadap layanan *mobile banking* mereka. Hal ini sejalan dengan teori Kotler, di mana keempat dimensi loyalitas saling terkait dan dipengaruhi oleh pengalaman nasabah dengan kebijakan dan layanan yang ditawarkan oleh lembaga keuangan. Kebijakan penanganan *cyber*

*crime* yang diterapkan oleh BSI Cabang Sinjai memiliki implikasi signifikan terhadap pembentukan dan pemeliharaan loyalitas nasabah. Philip Kotler, pakar pemasaran terkemuka, mengidentifikasi empat dimensi utama loyalitas, yaitu *repeat intention* (niat untuk menggunakan kembali), *word-of-mouth* (dari mulut ke mulut), *price sensitivity* (sensitivitas terhadap harga), dan *complaining behavior* (perilaku dalam menyampaikan keluhan). Kebijakan BSI dalam menangani *cyber crime* secara langsung maupun tidak langsung memengaruhi keempat dimensi ini.

## Saran

Berdasarkan hasil dan analisis yang telah dilakukan, penelitian ini masih banyak kekurangan dan kelemahan, sehingga masih banyak yang harus diperbaiki. Adapun saran yang ditujukan kepada peneliti selanjutnya: Bagi BSI Kabupaten Sinjai, sebaiknya mempertahankan bahkan meningkatkan kebijakan penanganan *cyber crime* pada pengguna *mobile banking* sebagai upaya mempertahankan loyalitas nasabah. Bagi peneliti selanjutnya, sebaiknya peneliti dapat memperluas ruang lingkup penelitian.

## DAFTAR PUSTAKA

Adila. (2017). *Pengaruh Layanan Mobile Banking Terhadap Kepuasan Pelanggan*.

Bahl, S. (2012). E-Banking : Challenges & Policy Implications. *Proceedings of 'I-Society 2012' at GKU, Talwandi Sabo Bathinda (Punjab)*, 1–12.

Barquin, S., Gantes, G. de, HV, V., & Shrikhande, D. (2019). Digital banking in Indonesia: Building loyalty and generating growth. *McKinsey & Company*, (February), 6.

Hidayatputra Pratama, T., & Nurhayati, I. (2023). *Perlindungan Nasabah Pengguna Layanan E-banking Dalam Perspektif Cybercrime*.

Mainata, D. (2018). Analytical Tools dan SWOT Analysis Penggunaan M-Banking Perbankan Syariah di Indonesia [Analytical Tools and SWOT Analysis The Use of M-Banking in Islamic Banking in Indonesia]. *Al-Tijary*, *3*(2), 160.

Miftahuddin, M., & Hendarsyah, D. (2019). Analisis Perbandingan Fasilitas Aplikasi Mobile Banking Bank Syariah Mandiri KCP. Bengkalis Dengan Bank Mandiri KC. Bengkalis. *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita*, *8*(1), 16–32. https://doi.org/10.46367/iqtishaduna.v8i1.149

Ni Nyoman Anita Candrawati. (2014). Perlindungan Hukum Terhadap ERLINDUNGAN HUKUM TERHADAP PEMEGANG KARTU E-MONEY SEBAGAI

ALAT PEMBAYARAN DALAM TRANSAKSI KOMERSIAL. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *3*(1), 1–16.

Oktaviani, G. (2019). Pengaruh Kepuasan Terhadap Loyalitas Pelanggan pada Jasa PT Gita Rifa Express (Studi Kasus Pengiriman Barang Daerah Batusangkar). *Universitas Islam Riau*, 10.

Purwani, M. S. F. (2023). Analisis Peran dan Penanggulangan Kejahatan Siber: Studi Kasus Spearphishing. *Restorative : Journal of Indonesian Probation and Parole System*, *1*(1), 33–45. https://doi.org/10.61682/restorative.v1i1.5

Sari, D. M., Fasa, M. I., & Suharto, S. (2021). Fitur-Fitur Aplikasi Mobile Banking Bank Syaraih. *Al-Infaq: Jurnal Ekonomi Islam*, *12*(2), 170.

See, B. R. (2022). Perlindungan Hukum Bagi Nasabah Dan Bank Terhadap Tindak Kejahatan Berbasis Teknologi Informasi (Cyber Crime). *Jurnal Hukum Caraka Justitia*, *2*(1), 54. https://doi.org/10.30588/jhcj.v2i1.1035

Syahputra, A. (2020). Analisis Kebijakan Dalam Penanganan Kejahatan Cyber Crime (Studi Kasus Cabang Bank BNI Syariah Lhokseumawe). *Paper Knowledge . Toward a Media History of Documents*, 12–26.

Utin Indah Permata Sari. (2022). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58–77. https://doi.org/10.61084/jsl.v2i01.7