KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.2, No.2 April 2025
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 151-162
DOI: https://doi.org/10.61722/jmia.v2i2.4223

TANTANGAN DAN STRATEGI PERLINDUNGAN KONSUMEN PADA LAYANAN PERBANKAN DI TENGAH KEMAJUAN TEKNOLOGI

Indryana Widi Ardhianty
Universitas Negeri Semarang

Alamat: Sekaran, Kec. Gn. Pati, Kota Semarang, Jawa Tengah 50229
Korespondensi penulis: widiantyindiii@gmail.com

Abstract. *This article discusses the challenges and consumer protection strategies in banking services in the era of technological advancement. The development of digital technology has brought significant changes in banking services, increasing accessibility and efficiency. However, this also poses new challenges related to data security, privacy, and the potential for fraud. This article analyzes various challenges faced by consumers, such as vulnerability to cyber attacks, lack of digital literacy, and the complexity of digital banking products. Furthermore, this article proposes effective consumer protection strategies, including strengthening regulations, increasing consumer education, and implementing advanced security technologies.*

Keywords: *Consumer Protection; Bank Services; Digital Literacy*

Abstrak. Artikel ini membahas tantangan dan strategi perlindungan konsumen dalam layanan perbankan di era kemajuan teknologi. Perkembangan teknologi digital telah membawa perubahan signifikan dalam layanan perbankan, meningkatkan aksesibilitas dan efisiensi. Namun, hal ini juga menimbulkan tantangan baru terkait keamanan data, privasi, dan potensi penipuan. Artikel ini menganalisis berbagai tantangan yang dihadapi konsumen, seperti kerentanan terhadap serangan siber, kurangnya literasi digital, dan kompleksitas produk perbankan digital. Selanjutnya, artikel ini mengusulkan strategi perlindungan konsumen yang efektif, termasuk penguatan regulasi, peningkatan edukasi konsumen, dan penerapan teknologi keamanan yang canggih.

Kata Kunci: Perlindungan Konsumen, Layanan Perbankan, Literasi Digital

PENDAHULUAN

Era industri 4.0 membawa transformasi mendalam bagi kehidupan manusia, mengubah cara berpikir, hidup, dan berinteraksi. Dampaknya terasa di berbagai sektor, termasuk teknologi, ekonomi, sosial, dan politik. Pelaku industri memanfaatkan teknologi digital sebagai modal untuk mengembangkan bisnis dan berkolaborasi mencapai tujuan bersama.

Dalam era modern ini, masyarakat luas telah mengakrabi teknologi, termasuk perkembangan teknologi di sektor perbankan. Penemuan komputer sebagai produk inovasi ilmu pengetahuan dan teknologi memicu konvergensi antara teknologi telekomunikasi, media, dan komputasi, yang menghasilkan medium baru bernama internet. Seiring waktu, internet telah menjadi kebutuhan esensial bagi sebagian besar entitas pemerintahan, aktivitas media sosial,

Received Maret, 2025; Revised Maret, 2025;April, 2025
*

perdagangan elektronik, serta dimanfaatkan dalam layanan perbankan untuk meningkatkan efisiensi dan kemudahan layanan publik.

Kemunculan internet telah mengubah paradigma komunikasi dan bisnis, mentransformasi aktivitas yang sebelumnya terbatas pada interaksi tatap muka atau fisik. Pertumbuhan pesat teknologi dan perkembangan digital saat ini turut mendorong perubahan dalam lanskap bisnis, khususnya di sektor perbankan.

Seiring dengan pergeseran pertumbuhan industri menuju digitalisasi, berbagai aktivitas mengalami transformasi sesuai dengan perkembangan yang ada. Inovasi teknologi yang memfasilitasi kehidupan juga merambah sektor keuangan. Salah satu sektor yang mengalami pergeseran menuju era industri 4.0 adalah perbankan. Industri perbankan merupakan sektor jasa yang berkembang pesat dan mampu mendorong pertumbuhan ekonomi Indonesia, mengingat perannya sebagai penyumbang pendapatan nasional dan lembaga intermediasi yang menghimpun dana masyarakat serta menyalurkannya kembali ke kegiatan ekonomi produktif.

Transformasi digital dalam industri perbankan melampaui penyediaan layanan daring atau perbankan seluler semata. Sektor keuangan perbankan perlu berinovasi dengan mengintegrasikan teknologi digital dengan interaksi nasabah, yang mana inovasi teknologi tersebut harus memfasilitasi dan memberikan kenyamanan bagi pengguna dalam mengakses layanan perbankan.

Transformasi digital dalam industri perbankan melampaui penyediaan layanan daring atau perbankan seluler semata. Sektor keuangan perbankan perlu berinovasi dengan mengintegrasikan teknologi digital dengan interaksi nasabah, yang mana inovasi teknologi tersebut harus memfasilitasi dan memberikan kenyamanan bagi pengguna dalam mengakses layanan perbankan.

Di Indonesia, sektor perbankan digital mencatatkan pertumbuhan pesat dalam beberapa tahun terakhir. Berdasarkan hasil survei yang dilakukan oleh Populix, pertumbuhan signifikan ini didorong oleh preferensi generasi Z yang berusia 12 hingga 27 tahun. Data dari Bank Indonesia (BI) menunjukkan bahwa nilai transaksi perbankan digital mencapai Rp 5.570,49 triliun pada Mei 2024, mengalami peningkatan tahunan sebesar 10,82%. Riset Populix yang berjudul "Studi Analisis Ekosistem dan Persepsi terhadap Bank Digital di Indonesia" mengidentifikasi beberapa faktor pendorong pertumbuhan ini, termasuk keamanan data dan transaksi (31%), fleksibilitas akses aplikasi (12%), kelengkapan fitur aplikasi (12%), integrasi dengan layanan keuangan lain (11%), dan penawaran promo khusus (10%). Tiga bank digital utama yang menjadi pilihan generasi Z adalah SeaBank (57% pangsa pasar), Bank Jago (36% pangsa pasar), dan Blu by BCA (26% pangsa pasar). Penggunaan utama bank digital meliputi pengisian ulang dompet elektronik (54%), transfer antar bank (49%), transaksi belanja di platform e-commerce atau daring (48%), serta transfer antar rekening (47%).

Meskipun layanan perbankan digital menawarkan berbagai kemudahan, terdapat tantangan signifikan terkait perlindungan konsumen. Risiko seperti kebocoran data pribadi, serangan siber, dan penipuan daring semakin mengkhawatirkan. Selain itu, tingkat pemahaman digital masyarakat yang bervariasi meningkatkan kerentanan konsumen terhadap kejahatan siber seperti phishing, skimming, dan rekayasa sosial. Oleh karena itu, inovasi teknologi di sektor perbankan harus diimbangi dengan upaya perlindungan konsumen yang kuat dan komprehensif.

Dalam layanan perbankan digital, regulator dan pelaku industri perbankan memiliki peran penting dalam membuat kebijakan yang menjamin keamanan, keterbukaan, dan keadilan. Peraturan yang mencakup perlindungan data pribadi, keamanan sistem teknologi informasi, dan

cara menangani keluhan pelanggan sangatlah krusial. Selain itu, upaya bank dalam meningkatkan pemahaman digital masyarakat juga merupakan strategi utama untuk mengurangi risiko kerugian pelanggan karena kurangnya pengetahuan akan potensi bahaya di dunia digital.

Layanan perbankan digital telah lama hadir di Indonesia, dan kerangka hukum di negara ini terus disesuaikan untuk mengakomodasi perkembangan tersebut. Mulai dari undang-undang, peraturan pemerintah, hingga peraturan yang dikeluarkan oleh otoritas pengawas perbankan, semua upaya ini bertujuan untuk memastikan bahwa layanan perbankan digital di Indonesia tetap mematuhi prinsip keamanan yang ketat, yang pada akhirnya melindungi nasabah yang menggunakan layanan tersebut.

METODE PENELITIAN

Pembahasan masalah yang dibahas dalam artikel ini dibahas dan dianalisis dengan memakai metode penelitian hukum yuridis normatif. Dalam artikel ini metode yang digunakan adalah metode penelitian yuridis normatif, yang akan berdasar pada norma hukum dalam beberapa peraturan dan menggunakan studi pustaka.

HASIL PENELITIAN DAN PEMBAHASAN

Strategi yang Diterapkan oleh Institusi Perbankan dalam Melindungi Konsumen pada Layanan Perbankan Digital di Era modernisasi Teknologi

Dalam era digital saat ini, perlindungan data dan privasi konsumen menjadi prioritas utama dalam layanan perbankan daring. Untuk menjaga keamanan informasi nasabah, lembaga perbankan menerapkan teknologi enkripsi ujung-ke-ujung (end-to-end) guna memastikan kerahasiaan data yang dikirimkan selama transaksi digital. Teknologi ini menjamin bahwa data yang ditransmisikan antara pengguna dan server bank tidak dapat diakses atau dimodifikasi oleh pihak yang tidak sah. Keamanan ujung-ke-ujung bergantung pada protokol dan mekanisme yang diimplementasikan pada titik akhir koneksi. Keamanan pada titik akhir ini memerlukan beberapa elemen penting, termasuk identitas, protokol, algoritma, implementasi, dan operasi yang aman.

Selain itu, untuk memperkuat keamanan dalam proses otentikasi pengguna, sistem Otentikasi Multi-Faktor (MFA) diterapkan. MFA menggabungkan beberapa tingkatan keamanan, seperti penggunaan kata sandi, kode OTP (Kata Sandi Sekali Pakai), atau perangkat token. Teknologi biometrik, seperti pengenalan sidik jari, wajah, atau retina mata, juga semakin sering digunakan oleh bank untuk memastikan bahwa hanya pemilik akun yang dapat mengakses layanan digital mereka. Kombinasi berbagai metode otentikasi ini tidak hanya meningkatkan lapisan perlindungan, tetapi juga mengurangi risiko akses ilegal yang mungkin terjadi jika hanya mengandalkan kata sandi.

Lembaga perbankan diwajibkan untuk mematuhi kebijakan privasi data yang sesuai dengan regulasi baik nasional maupun internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia. Kebijakan ini mengatur cara pengumpulan, penyimpanan, dan penggunaan data pribadi nasabah oleh bank. Kepatuhan terhadap regulasi ini bukan hanya kewajiban hukum, tetapi juga menjadi penentu kepercayaan nasabah terhadap lembaga perbankan. Regulasi tersebut mengharuskan bank untuk memberikan informasi yang transparan mengenai penggunaan data dan memberikan hak kepada nasabah untuk mengakses atau meminta penghapusan data mereka.

Salah satu tantangan utama dalam layanan perbankan digital adalah ancaman penipuan atau *fraud*. Oleh karena itu, bank semakin banyak mengandalkan sistem berbasis kecerdasan

buatan (AI) untuk mendeteksi dan mencegah aktivitas mencurigakan. AI mampu menganalisis pola transaksi nasabah secara *real-time* dan memberikan peringatan jika ada aktivitas yang tidak sesuai dengan pola normal. Misalnya, transaksi besar yang tiba-tiba dilakukan dari lokasi yang tidak biasa dapat langsung dihentikan sementara oleh sistem hingga pengguna mengonfirmasi keabsahan transaksi tersebut. Dengan pendekatan ini, bank dapat merespons ancaman dengan cepat sebelum kerugian yang lebih besar terjadi. Di sisi lain, teknologi yang digunakan juga harus mampu melindungi dari ancaman serangan siber, seperti *phishing*, *malware*, atau serangan *ransomware*. Oleh karena itu, penguatan sistem keamanan melalui pembaruan perangkat lunak secara berkala menjadi suatu keharusan. Sistem perbankan digital yang tidak diperbarui akan lebih rentan terhadap eksploitasi oleh penyerang yang memanfaatkan celah keamanan. Selain itu, bank juga perlu bekerja sama dengan penyedia layanan keamanan siber untuk memastikan bahwa mereka memiliki perlindungan terbaru terhadap ancaman yang terus berkembang.

Dalam konteks perlindungan data, bank juga bertanggung jawab untuk memastikan keamanan sistem penyimpanan data mereka dari potensi kebocoran. Informasi sensitif seperti nomor rekening, detail kartu kredit, atau data biometrik harus disimpan dalam format terenkripsi di server yang dilindungi secara fisik dan digital. Selain itu, penerapan kebijakan kontrol akses berbasis peran (Role-Based Access Control) dapat membatasi akses data hanya kepada pihak yang berwenang, sehingga mengurangi risiko kebocoran dari dalam. Bank juga memiliki kewajiban untuk mengedukasi nasabah tentang pentingnya menjaga keamanan data pribadi mereka. Banyak kasus pencurian data terjadi karena kelalaian nasabah, seperti memberikan informasi pribadi kepada pihak yang tidak dikenal atau mengabaikan peringatan keamanan. Kampanye kesadaran mengenai ancaman digital dan cara menghindarinya, seperti tidak mengklik tautan mencurigakan atau tidak membagikan OTP kepada siapa pun, menjadi langkah penting dalam melindungi konsumen.

Melalui kombinasi teknologi, regulasi, dan edukasi, lembaga perbankan berupaya menciptakan ekosistem layanan digital yang aman dan dapat dipercaya. Namun, keamanan data dan privasi merupakan upaya berkelanjutan yang memerlukan investasi konstan dalam teknologi dan kebijakan baru untuk menghadapi ancaman yang terus berkembang. Keberhasilan dalam melindungi konsumen tidak hanya mencerminkan kualitas layanan perbankan, tetapi juga memperkuat kepercayaan masyarakat terhadap lembaga keuangan di era digital.

Pendidikan dan literasi digital bagi konsumen merupakan elemen penting dalam menciptakan ekosistem perbankan digital yang aman dan efisien. Salah satu langkah utama yang diambil lembaga perbankan adalah menyelenggarakan kampanye kesadaran keamanan digital. Kampanye ini bertujuan untuk mengedukasi konsumen mengenai berbagai ancaman di dunia digital, seperti *phishing*, *malware*, dan penipuan daring. Dalam kampanye ini, bank biasanya memberikan informasi tentang cara mengenali surel atau pesan mencurigakan yang sering digunakan dalam serangan *phishing*, menghindari pengunduhan perangkat lunak dari sumber yang tidak tepercaya, serta pentingnya tidak membagikan informasi sensitif seperti OTP atau PIN kepada siapa pun, termasuk pihak yang mengaku sebagai pegawai bank. Selain melalui iklan, media sosial, atau situs web resmi, bank juga sering bekerja sama dengan lembaga lain seperti regulator atau lembaga pendidikan untuk memperluas jangkauan kampanye dan menjangkau masyarakat yang kurang terpapar teknologi.

Selain kampanye kesadaran, pelatihan penggunaan aplikasi perbankan digital juga menjadi fokus dalam edukasi digital konsumen. Bank menyediakan berbagai sarana pembelajaran, seperti video tutorial, panduan langkah demi langkah di situs web, dan webinar interaktif, untuk membantu nasabah memahami cara menggunakan layanan digital mereka

dengan aman. Pelatihan ini mencakup berbagai topik, mulai dari cara mengunduh dan menginstal aplikasi resmi, melakukan login dengan otentikasi yang aman, hingga memanfaatkan fitur-fitur seperti transfer dana, pembayaran tagihan, atau pengaturan notifikasi keamanan. Bank juga memberikan simulasi penggunaan aplikasi untuk meningkatkan kepercayaan diri nasabah dalam mengoperasikan layanan digital. Dengan adanya pelatihan ini, tidak hanya nasabah yang melek teknologi yang merasa nyaman menggunakan layanan digital, tetapi juga mereka yang baru pertama kali mengakses teknologi perbankan. Langkah ini penting untuk memastikan inklusi keuangan sekaligus meminimalkan risiko kesalahan yang dapat menyebabkan kerugian bagi konsumen.

Regulasi dan kepatuhan terhadap hukum menjadi dasar utama dalam menjaga keamanan dan kepercayaan konsumen dalam layanan perbankan digital. Salah satu langkah penting yang diambil oleh lembaga perbankan adalah penerapan standar keamanan internasional, seperti ISO 27001, yang merupakan standar global untuk manajemen keamanan informasi. Sertifikasi ini memastikan bahwa bank memiliki sistem pengelolaan risiko yang efektif untuk melindungi data sensitif nasabah dari ancaman eksternal maupun internal. Dengan standar ini, bank harus mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan secara sistematis, mencakup perlindungan data pribadi hingga infrastruktur teknologi yang digunakan. Kepatuhan terhadap standar ini tidak hanya menunjukkan komitmen bank terhadap keamanan, tetapi juga memberikan jaminan kepada konsumen bahwa data mereka dilindungi sesuai dengan praktik terbaik internasional.

Selain mematuhi standar internasional, lembaga perbankan juga wajib mengikuti regulasi yang ditetapkan oleh pemerintah, seperti peraturan dari Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK). Regulasi ini mencakup berbagai aspek perlindungan konsumen digital, termasuk kewajiban bank untuk memberikan informasi yang transparan mengenai layanan digital, pengelolaan risiko transaksi elektronik, serta pelaporan insiden keamanan siber kepada regulator. Regulasi ini dirancang untuk melindungi konsumen dari risiko penyalahgunaan data, penipuan, dan kegagalan sistem yang dapat merugikan nasabah. Di Indonesia, misalnya, Undang-Undang Perlindungan Data Pribadi (UU PDP) menjadi dasar hukum yang mengatur bagaimana data nasabah harus dikumpulkan, digunakan, dan disimpan dengan aman. Dengan mematuhi regulasi ini, bank tidak hanya memenuhi kewajiban hukum tetapi juga membangun kepercayaan publik terhadap layanan digital mereka.

Pengawasan internal dan audit keamanan digital menjadi langkah selanjutnya untuk memastikan bahwa regulasi dan standar yang diterapkan dijalankan secara konsisten. Lembaga perbankan melakukan evaluasi berkala terhadap keamanan sistem mereka melalui audit internal maupun eksternal. Audit ini mencakup pemeriksaan terhadap protokol keamanan, mekanisme otentikasi, enkripsi data, serta prosedur manajemen insiden keamanan. Pengawasan internal yang efektif memastikan bahwa setiap potensi celah keamanan dapat diidentifikasi dan ditangani sebelum menjadi ancaman yang lebih besar. Selain itu, bank juga sering kali menggunakan pihak ketiga yang independen untuk melakukan audit keamanan, memberikan perspektif objektif tentang sejauh mana sistem mereka mampu melindungi data konsumen. Langkah ini penting untuk menjaga integritas operasional bank sekaligus memastikan bahwa layanan digital tetap berada dalam standar yang diharapkan oleh konsumen dan regulator.

Dalam menghadapi tantangan era digital, bank berfokus pada pengembangan teknologi yang berpusat pada konsumen untuk meningkatkan pengalaman pengguna. Salah satu inovasi utama adalah menciptakan aplikasi perbankan yang ramah pengguna, dengan desain intuitif yang mudah digunakan oleh semua kalangan, termasuk generasi muda yang terbiasa dengan teknologi

dan generasi tua yang relatif baru mengenal layanan digital. Desain antarmuka yang sederhana memungkinkan nasabah untuk mengakses informasi rekening, melakukan transfer dana, atau membayar tagihan dengan langkah yang jelas dan mudah dipahami. Selain itu, bank juga memastikan bahwa aplikasi dapat diakses oleh penyandang disabilitas melalui fitur seperti teks besar, pembaca layar, atau navigasi berbasis suara. Upaya ini memastikan inklusivitas sekaligus memberikan kenyamanan bagi berbagai lapisan masyarakat.

Di sisi lain, kehadiran *chatbot* AI dan layanan pelanggan 24/7 menjadi solusi praktis dalam memberikan bantuan langsung kepada nasabah. *Chatbot* AI dirancang untuk menjawab pertanyaan sederhana, seperti mengecek saldo, memberikan informasi lokasi cabang terdekat, atau menjelaskan prosedur tertentu tanpa melibatkan staf manusia. Untuk masalah yang lebih kompleks, layanan pelanggan yang tersedia sepanjang waktu melalui *live chat* atau panggilan telepon memungkinkan nasabah mendapatkan solusi kapan saja, bahkan di luar jam operasional tradisional. Inovasi ini tidak hanya meningkatkan efisiensi, tetapi juga memberikan rasa aman kepada konsumen bahwa mereka selalu bisa mendapatkan dukungan saat dibutuhkan.

Selain itu, penyesuaian layanan sesuai kebutuhan individu menjadi salah satu strategi utama yang diterapkan oleh bank untuk memenuhi preferensi spesifik konsumen. Dengan memanfaatkan analisis data, bank mampu memberikan rekomendasi keuangan yang relevan berdasarkan kebiasaan transaksi dan tujuan keuangan masing-masing nasabah. Misalnya, nasabah yang sering berbelanja daring mungkin akan ditawari program kartu kredit dengan pengembalian dana khusus untuk transaksi perdagangan elektronik, sementara nasabah yang fokus pada investasi akan mendapatkan informasi tentang produk investasi yang sesuai dengan profil risiko mereka. Pendekatan yang disesuaikan ini tidak hanya meningkatkan kepuasan nasabah, tetapi juga memperkuat hubungan jangka panjang antara bank dan konsumen.

Mekanisme penyelesaian keluhan dan pengaduan menjadi elemen penting dalam membangun kepercayaan konsumen terhadap layanan perbankan digital. Bank menyediakan pusat layanan pelanggan berupa saluran telepon atau dukungan obrolan yang responsif untuk menangani keluhan secara langsung. Melalui saluran ini, nasabah dapat melaporkan masalah, seperti transaksi yang gagal atau tagihan yang tidak sesuai, dan mendapatkan respons cepat dari tim yang kompeten. Pusat layanan ini dirancang untuk memberikan pengalaman yang ramah dan solutif, di mana petugas dilatih untuk mendengarkan keluhan dengan empati dan menawarkan solusi yang sesuai dengan kebutuhan nasabah. Lebih lanjut, sistem resolusi sengketa digital menjadi alternatif yang semakin populer dalam menyelesaikan masalah nasabah dengan cepat. Dengan platform ini, konsumen tidak perlu datang ke kantor cabang atau mengirim dokumen secara fisik, melainkan dapat mengajukan pengaduan secara daring melalui aplikasi atau situs web resmi bank. Sistem ini memungkinkan pengolahan pengaduan secara otomatis, termasuk pelacakan status kasus, komunikasi langsung dengan pihak yang menangani, dan pemberian solusi secara transparan. Pendekatan digital ini sangat efisien, terutama bagi nasabah yang tinggal di daerah terpencil atau memiliki mobilitas terbatas.

Keterbukaan dalam penyelesaian masalah juga menjadi prioritas utama bagi bank untuk menjaga kepercayaan konsumen. Nasabah diberikan laporan perkembangan kasus secara berkala, termasuk langkah-langkah yang telah diambil dan perkiraan waktu penyelesaian. Jika pengaduan tidak dapat diselesaikan dalam waktu yang diharapkan, nasabah juga diberi penjelasan yang rinci mengenai alasan keterlambatan dan solusi alternatif yang tersedia. Dengan adanya keterbukaan ini, nasabah merasa dihargai dan lebih percaya bahwa bank berkomitmen untuk melindungi hak-hak mereka sebagai konsumen. Melalui pengembangan teknologi yang berorientasi konsumen dan sistem penanganan keluhan yang responsif, bank tidak hanya menciptakan pengalaman yang

lebih nyaman bagi nasabah, tetapi juga memperkuat posisi mereka sebagai lembaga yang dapat diandalkan di era digital. Hal ini penting untuk menjaga loyalitas konsumen sekaligus menghadapi persaingan ketat di industri perbankan modern.

Kepercayaan konsumen terhadap lembaga perbankan sangat bergantung pada tingkat keterbukaan dalam layanan yang diberikan. Bank perlu menyampaikan informasi yang jelas dan rinci terkait biaya, syarat, dan ketentuan layanan. Misalnya, biaya administrasi, bunga pinjaman, atau batasan transaksi harus dijelaskan secara terbuka baik melalui aplikasi, situs web, maupun dokumen kontrak. Dengan memberikan informasi ini secara transparan, konsumen dapat membuat keputusan yang lebih sadar dan merasa yakin bahwa tidak ada biaya tersembunyi yang membebani mereka. Keterbukaan ini menjadi dasar penting dalam menciptakan hubungan yang sehat antara bank dan nasabah.

Langkah selanjutnya adalah mengadakan audit publik secara berkala, di mana bank mempublikasikan laporan tentang langkah-langkah keamanan dan operasional yang mereka lakukan. Laporan ini tidak hanya membahas kinerja keuangan, tetapi juga langkah konkret yang diambil untuk melindungi data konsumen, seperti pembaruan sistem keamanan atau respons terhadap insiden siber. Dengan melibatkan publik dalam pengawasan ini, bank menunjukkan komitmen mereka terhadap akuntabilitas, yang dapat memperkuat citra lembaga di mata konsumen.

Sertifikasi keamanan digital juga memainkan peran penting dalam meningkatkan kepercayaan konsumen. Pengakuan dari lembaga terpercaya seperti ISO 27001 atau Payment Card Industry Data Security Standard (PCI DSS) menunjukkan bahwa bank telah memenuhi standar global dalam melindungi data konsumen. Sertifikasi ini memberikan jaminan tambahan bahwa bank tidak hanya mematuhi regulasi lokal, tetapi juga menerapkan praktik terbaik internasional dalam manajemen keamanan.

Dalam menghadapi tantangan keamanan digital, kolaborasi dengan perusahaan keamanan siber menjadi langkah strategis yang diambil oleh banyak bank. Kemitraan ini memungkinkan bank untuk mengadopsi teknologi keamanan terbaru yang dirancang untuk melindungi data dan transaksi konsumen. Perusahaan keamanan siber menyediakan solusi seperti sistem deteksi ancaman berbasis AI, firewall tingkat lanjut, hingga layanan mitigasi serangan DDoS. Dengan menggandeng ahli keamanan, bank dapat fokus pada pengembangan layanan utama mereka tanpa mengabaikan aspek keamanan.

Peningkatan infrastruktur teknologi awan juga merupakan bagian dari kolaborasi dengan penyedia layanan awan yang aman. Teknologi awan memungkinkan bank untuk menyimpan dan mengolah data dalam skala besar dengan efisiensi tinggi, sambil memastikan tingkat keamanan yang optimal. Penyedia layanan awan biasanya dilengkapi dengan protokol keamanan yang canggih, termasuk enkripsi data dan redundansi sistem untuk mencegah kehilangan data. Dengan memanfaatkan teknologi ini, bank tidak hanya meningkatkan kecepatan layanan, tetapi juga memastikan data konsumen tetap aman. Selain itu, kolaborasi dengan platform *fintech* membantu bank menciptakan ekosistem digital yang terintegrasi. *Fintech* sering kali menawarkan solusi inovatif seperti dompet digital, pinjaman *peer-to-peer*, atau pembayaran instan yang melengkapi layanan perbankan tradisional. Integrasi ini memungkinkan nasabah untuk mengakses berbagai layanan keuangan dari satu platform, menciptakan pengalaman yang lebih praktis dan lancar. Dalam ekosistem ini, bank dan *fintech* dapat saling melengkapi untuk memberikan nilai tambah kepada konsumen.

Teknologi *big data* dan kecerdasan buatan (AI) semakin sering dimanfaatkan untuk meningkatkan keamanan dan pengelolaan risiko dalam perbankan digital. Dengan analisis data

dalam jumlah besar, bank dapat memprediksi pola aktivitas mencurigakan yang mengindikasikan potensi ancaman, seperti upaya penipuan atau akses ilegal. Sistem ini mampu memproses ribuan transaksi dalam waktu singkat untuk mengidentifikasi anomali, seperti transaksi besar yang dilakukan dari lokasi geografis yang tidak biasa. Deteksi dini ini memungkinkan bank untuk mengambil tindakan pencegahan sebelum ancaman berkembang menjadi lebih serius. AI juga memainkan peran penting dalam pengelolaan risiko, terutama dalam mengurangi ancaman secara otomatis. Sistem berbasis AI dapat mempelajari pola serangan siber dan terus memperbarui strategi perlindungan tanpa campur tangan manusia. Misalnya, jika AI mendeteksi serangan *phishing* yang menargetkan sejumlah besar nasabah, sistem dapat langsung memblokir tautan berbahaya dan memperingatkan konsumen melalui aplikasi atau email. Pendekatan ini tidak hanya mengurangi risiko, tetapi juga meningkatkan efisiensi operasional. Salah satu tantangan utama yang dihadapi lembaga perbankan di era modernisasi teknologi adalah meningkatnya serangan siber. Ancaman seperti *phishing*, *ransomware*, atau serangan DDoS dapat mengganggu operasional bank dan membahayakan data konsumen. Untuk mengatasi hal ini, bank harus terus memperbarui infrastruktur keamanan mereka, termasuk mengadopsi teknologi AI, meningkatkan pelatihan keamanan bagi karyawan, dan bekerja sama dengan regulator untuk memperketat regulasi keamanan siber.

Efektivitas Strategi dan Kebijakan yang Ada dalam Menjamin Keamanan dan Kepercayaan Konsumen pada Layanan Perbankan Digital

Penelitian ini menyimpulkan bahwa efektivitas strategi dan kebijakan perlindungan konsumen dalam layanan perbankan digital bervariasi dalam menjamin keamanan dan kepercayaan konsumen. Salah satu strategi utama yang diidentifikasi adalah penerapan teknologi keamanan seperti enkripsi data, otentikasi dua faktor, dan sistem deteksi penipuan yang canggih. Kebijakan regulasi yang ketat dari otoritas perbankan dan keuangan juga memainkan peran penting dalam mengatur dan memastikan kepatuhan bank terhadap standar keamanan. Namun, masih terdapat beberapa kekurangan, seperti kurangnya edukasi konsumen mengenai keamanan digital dan terbatasnya transparansi kebijakan perlindungan data.

Strategi keamanan digital yang diterapkan oleh bank memiliki peran penting dalam melindungi konsumen dari ancaman siber. Menurut teori keamanan informasi oleh Whitman dan Mattord (2018), strategi keamanan yang efektif melibatkan kebijakan, teknologi, dan prosedur yang dirancang untuk melindungi informasi dari ancaman yang disengaja maupun tidak disengaja. Temuan penelitian ini menunjukkan bahwa penggunaan enkripsi data dan otentikasi dua faktor sejalan dengan teori ini, yang menekankan pentingnya lapisan-lapisan perlindungan untuk menjaga integritas dan kerahasiaan data konsumen. Enkripsi data merupakan proses mengubah data menjadi kode rahasia yang hanya dapat dibaca oleh pihak yang memiliki kunci enkripsi. Dengan demikian, enkripsi melindungi data konsumen dari akses ilegal selama transmisi dan penyimpanan.

Selain itu, peraturan dari otoritas perbankan seperti Bank Indonesia dan Otoritas Jasa Keuangan (OJK) memiliki peran krusial dalam memastikan bank mematuhi standar keamanan. Berdasarkan Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, bank diwajibkan untuk menyediakan mekanisme perlindungan yang memadai bagi konsumen. Peraturan ini bertujuan untuk memastikan bahwa bank mengimplementasikan praktik terbaik dalam perlindungan data konsumen dan merespons insiden keamanan dengan cepat dan

efisien. Peraturan ini juga mengharuskan bank untuk menyusun kebijakan keamanan informasi yang mencakup pengelolaan risiko, pencegahan, deteksi, dan respons terhadap insiden keamanan.

Namun, penelitian ini juga menemukan bahwa edukasi konsumen masih kurang memadai. Berdasarkan teori perlindungan konsumen oleh Day dan Aaker (1997), edukasi konsumen adalah elemen kunci dalam meningkatkan kepercayaan konsumen terhadap layanan perbankan digital. Konsumen yang memahami langkah-langkah keamanan yang perlu diambil dapat lebih efektif melindungi diri mereka dari penipuan dan serangan siber. Oleh karena itu, bank perlu meningkatkan upaya mereka dalam mengedukasi konsumen mengenai keamanan digital dan kebijakan perlindungan data. Edukasi konsumen dapat dilakukan melalui berbagai saluran, termasuk kampanye media sosial, seminar, webinar, dan materi edukasi yang tersedia di situs web bank.

Hasil penelitian menunjukkan bahwa meskipun strategi dan kebijakan yang ada sudah cukup kuat dalam menjamin keamanan data konsumen, masih ada beberapa area yang perlu ditingkatkan untuk memperkuat kepercayaan konsumen. Salah satu rekomendasi utama adalah peningkatan edukasi konsumen melalui kampanye informasi dan program pelatihan yang berfokus pada keamanan digital. Bank juga perlu meningkatkan transparansi kebijakan perlindungan data mereka dengan menyediakan informasi yang jelas dan mudah diakses oleh konsumen. Transparansi ini dapat mencakup penjelasan tentang bagaimana data konsumen dikumpulkan, digunakan, disimpan, dan dilindungi oleh bank.

Selain itu, kerja sama antara bank, otoritas regulasi, dan penyedia teknologi keamanan perlu diperkuat untuk memastikan bahwa semua pihak terlibat dalam upaya perlindungan konsumen. Teknologi keamanan harus terus diperbarui sesuai dengan perkembangan ancaman siber yang semakin kompleks. Bank juga harus memastikan bahwa mereka memiliki rencana respons insiden yang efektif untuk mengatasi dan meminimalkan dampak dari insiden keamanan. Rencana respons insiden ini harus mencakup langkah-langkah untuk mendeteksi insiden, memberitahu pihak terkait, mengatasi insiden, dan memulihkan sistem ke kondisi normal.

Dalam menghadapi era modernisasi teknologi, bank harus terus berinovasi dalam strategi keamanan mereka untuk mengatasi ancaman baru yang muncul. Hal ini mencakup investasi dalam teknologi terbaru seperti kecerdasan buatan dan *machine learning* untuk deteksi dan pencegahan penipuan. Teknologi ini memungkinkan bank untuk mengidentifikasi pola dan anomali yang mencurigakan dalam transaksi keuangan, sehingga dapat mencegah penipuan sebelum terjadi. Kepercayaan konsumen terhadap layanan perbankan digital dapat ditingkatkan dengan memastikan bahwa bank selalu berada di garis depan dalam hal keamanan dan perlindungan data.

Menurut teori perlindungan data oleh Solove (2006), pengumpulan, penyimpanan, dan penggunaan data konsumen harus dilakukan dengan transparansi dan tanggung jawab. Bank harus menjamin bahwa data konsumen dilindungi dari akses ilegal dan digunakan sesuai dengan persetujuan konsumen. Kebijakan privasi yang jelas dan komprehensif dapat membantu meningkatkan kepercayaan konsumen terhadap layanan perbankan digital. Selain itu, bank harus memiliki mekanisme untuk menangani pelanggaran data dengan cepat dan efisien, serta memberikan pemberitahuan kepada konsumen jika terjadi insiden keamanan.

Selain teknologi, kepercayaan konsumen juga dapat ditingkatkan melalui peningkatan transparansi dalam kebijakan perlindungan data. Bank harus menyediakan informasi yang jelas dan mudah diakses tentang bagaimana data konsumen dikumpulkan, digunakan, disimpan, dan dilindungi. Penjelasan ini harus mencakup hak-hak konsumen terkait data pribadi mereka, serta langkah-langkah yang diambil oleh bank untuk

melindungi data tersebut. Dengan memberikan transparansi ini, bank dapat membangun kepercayaan konsumen dan mengurangi kekhawatiran terkait privasi dan keamanan data.

Untuk mengatasi kurangnya edukasi konsumen, bank perlu mengembangkan program edukasi yang komprehensif tentang keamanan digital. Program ini dapat mencakup pelatihan tentang cara mengenali penipuan online, pentingnya menggunakan kata sandi yang kuat, dan langkah-langkah yang dapat diambil untuk melindungi informasi pribadi. Edukasi ini dapat dilakukan melalui berbagai saluran, termasuk seminar, webinar, video tutorial, dan materi edukasi yang tersedia di situs web bank. Dengan meningkatkan kesadaran dan pemahaman konsumen tentang keamanan digital, bank dapat membantu mereka melindungi diri dari ancaman siber.

Dalam menghadapi era modernisasi teknologi, bank harus terus berinovasi dalam strategi keamanan mereka. Ini termasuk investasi dalam teknologi terbaru, serta pengembangan kebijakan dan prosedur yang efektif untuk melindungi data konsumen. Bank juga perlu memastikan bahwa mereka memiliki rencana respons insiden yang efektif untuk menanggulangi dan memitigasi dampak dari insiden keamanan. Rencana respons ini harus mencakup langkah-langkah untuk mendeteksi insiden, memberitahu pihak terkait, mengatasi insiden, dan mengembalikan sistem ke kondisi normal.

Efektivitas strategi dan kebijakan perlindungan konsumen pada layanan perbankan digital tergantung pada kombinasi yang efektif dari teknologi keamanan, regulasi yang ketat, dan edukasi konsumen. Bank harus terus beradaptasi dengan perubahan lanskap teknologi dan ancaman siber untuk menjaga keamanan dan kepercayaan konsumen. Melalui upaya kolaboratif dan inovatif, perlindungan hak-hak konsumen dalam layanan perbankan digital dapat terjamin secara efektif. Keberhasilan kolaborasi ini sangat bergantung pada komitmen semua pihak dalam mengimplementasikan strategi keamanan yang mutakhir dan kebijakan perlindungan yang menyeluruh. Edukasi konsumen tentang pentingnya keamanan digital harus terus ditingkatkan, dengan menyediakan informasi yang jelas dan mudah diakses. Dengan demikian, konsumen dapat memahami bagaimana melindungi informasi pribadi mereka dan mengenali tanda-tanda potensi penipuan.

Kerjasama antara bank, otoritas regulasi, dan penyedia teknologi keamanan merupakan kunci dalam menciptakan ekosistem perbankan digital yang aman dan terpercaya. Otoritas regulasi harus terus memperbarui kebijakan dan regulasi untuk mengakomodasi perkembangan teknologi dan ancaman baru. Bank perlu memastikan bahwa mereka mematuhi standar yang ditetapkan dan terus memperbarui sistem keamanan mereka. Penyedia teknologi, di sisi lain, harus terus berinovasi untuk menyediakan solusi keamanan yang efektif dan mudah diintegrasikan dalam sistem perbankan.

Efektivitas strategi dan kebijakan perlindungan konsumen pada layanan perbankan digital tergantung pada kombinasi yang efektif dari teknologi keamanan, regulasi yang ketat, dan edukasi konsumen. Melalui upaya kolaboratif dan inovatif, bank, otoritas regulasi, dan penyedia teknologi dapat bersama-sama menciptakan lingkungan perbankan digital yang aman dan terpercaya. Keberhasilan ini tidak hanya akan

meningkatkan keamanan dan kepercayaan konsumen, tetapi juga mendukung pertumbuhan dan keberlanjutan industri perbankan digital di masa depan. Dengan teknologi yang lebih canggih, kebijakan yang lebih ketat, dan peningkatan kesadaran masyarakat, diharapkan upaya perlindungan hak konsumen di era digital dapat berjalan lebih efektif. Melalui kolaborasi yang erat antara berbagai pemangku kepentingan, perlindungan hak kekayaan intelektual dalam layanan perbankan digital dapat ditingkatkan dan memberikan manfaat yang lebih besar bagi industri perbankan serta masyarakat luas. Bank harus terus beradaptasi dengan perubahan lanskap teknologi dan ancaman siber untuk menjaga keamanan dan kepercayaan konsumen.

KESIMPULAN

Transformasi digital dalam perbankan memberikan berbagai manfaat, termasuk kemudahan akses dan efisiensi, tetapi juga menghadirkan tantangan seperti ancaman keamanan data, serangan siber, dan rendahnya literasi digital masyarakat. Untuk mengatasi tantangan ini, bank mengadopsi teknologi canggih seperti enkripsi data, autentikasi multi-faktor, dan sistem deteksi berbasis kecerdasan buatan. Regulasi seperti Undang-Undang Perlindungan Data Pribadi di Indonesia juga berperan penting dalam menjaga keamanan konsumen melalui penerapan standar perlindungan yang ketat.

Namun, meskipun strategi keamanan dan regulasi telah diterapkan, edukasi konsumen dan transparansi kebijakan perlindungan data masih perlu ditingkatkan. Bank perlu mengedukasi masyarakat tentang keamanan digital melalui kampanye dan pelatihan yang komprehensif. Selain itu, kolaborasi antara bank, otoritas regulasi, dan penyedia teknologi menjadi kunci untuk menciptakan ekosistem layanan perbankan digital yang aman dan terpercaya. Dengan kombinasi strategi ini, perlindungan konsumen dapat diperkuat, sehingga mendukung pertumbuhan industri perbankan digital secara berkelanjutan.

DAFTAR PUSTAKA

Abubakar, Lastuti, and Tri Handayani. "PENGUATAN REGULASI: UPAYA PERCEPATAN TRANSFORMASI DIGITAL PERBANKAN DI ERA EKONOMI DIGITAL." *JURNAL MASALAH-MASALAH HUKUM* 51, no. 3 (2022).

Ardianingsih, Arum, and Doddy Setiawan. *Audit Internal Berbasis Risiko*. PT Bumi Aksara, 2023.

Azizah, Rizka, Revana Aggraeni, and Yowa Selvia Bayu Mustika. "Peran Perlindungan Konsumen Dalam Era Digitalisasi Perbankan Bagi Konsumen." *OPTIMAL: Jurnal Ekonomi Dan Manajemen* 4, no. 2 (2024).

Gading, Samuel. "Hasil Survei: Bank Digital RI Tumbuh Pesat Gegara Gen Z." Detikfinance, 2024.

K.K, Azizah Shodiqoh Rafidah, and Happy Novasila Maharani. "INOVASI DAN PENGEMBANGAN PRODUK KEUANGAN SYARIAH: TANTANGAN DAN PROSPEK DI ERA REVOLUSI INDUSTRI 4.0." *JURNAL ILMIAH EDUNOMIKA*, 2024.

Kawengian, Violeta Michiko. "TINJAUAN HUKUM PERAN BANK SENTRAL TERHADAP PENGGUNAAN TEKNOLOGI BLOCKCHAIN DALAM

TRANSAKSI KEUANGAN DI INDONESIA." *Lex Privatum*, 2024.

Mandasari, Puti. "Analisis Faktor Layanan M-Banking Terhadap Kepuasan Nasabah Di Bank Syariah Indonesia KC Mamuju." INSTITUT AGAMA ISLAM NEGERI (IAIN), 2024.

Muhtadien, A. Zeze, Abdul Aziz, and Hendrik Hermawan. "Analisis Penguatan Digitalisasi Perbankan Melalui Peningkatan Perlindungan Dana Bank Konsumen Oleh OJK." *Jurnal Ekonomi, Akuntansi, Dan Perpajakan (JEAP)* 1, no. 3 (2024).

MURDIONO. "PENYUSUSNAN KEBIJAKAN KEAMANAN INFORMASI DENGEN PENILAIAN RISIKO KEAMANAN ASET PADA KAMPUS INSTITUT TEKNOLOGI SEPULUH NOPEMBER BERDASARKAN STANDAR ISO 27001." INSTITUT TEKNOLOGI SEPULUH NOPEMBER, 2020.

Pramukantoro, Eko Sakti, Fariz Andri Bakhtiar, Ahmad Lutfi Bayu Aji, and Deny Hari Prasetya Dewa. "IMPLEMENTASI MEKANISME END-TO-END SECURITY PADA IoT MIDDLEWARE." *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, 2019.

Putra, Denis Megel. "Perlindungan Hukum Terhadap Nasabah Pada Perbankan Digital." *Jurnal Ekonomu Bisnis, Manajemen Dan Akuntansi (JEBMAK)* 1, no. 1 (2022).

Santoso, Joseph Teguh. *Aplikasi AI Dan Machine Learning Dalam Bisnis*. Penerbit Yayasan Prima Agus Teknik, 2023.

Sirait, Rian Mangapul, Roy Fachraby Ginting, and Chris Dayanti Br Ginting. "TANTANGAN HUKUM PENGGUNAAN DATA BIOMETRIK DALAM KEPERLUAN BISNIS." *Jurnal Konseling Pendidikan Islam*, 2023.

Suari, Kadek Rima Anggen, and I Made Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum*, 2023.

Yustisia, Melia Prabangasta. "PERLINDUNGAN BA PERLINDUNGAN BAGI NASABAH D ASABAH DALAM PENYELENGGARAAN YELENGGARAAN LAYANAN PERBANKAN DIGI AN PERBANKAN DIGITAL DI INDONESI AL DI INDONESIA." *"Dharmasisya" Jurnal Program Magister Hukum FHUI* 2, no. 2.