CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 8 No 4 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

KEWAJIBAN HUKUM PERBANKAN DI INDONESIA DALAM MENJAMIN KEAMANAN TRANSAKSI DAN NASABAH DI ERA DIGITAL (STUDI KASUS SERANGAN SIBER BANK SYARIAH INDONESIA)

Fradisa Prabu Khairatthariq
Universitas Islam Negeri Sunan Gunung Djati Bandung
Email: fradisaprabukh24@gmail.com

ABSTRACT

This study aims to assess banks' legal obligations to safeguard consumers utilizing digital banking services. Additionally, the Indonesian digital banking scenario will be studied, with a focus on steps that might be taken to strengthen system security. A library research approach, which relies on secondary data or library materials, is used in this study. In this case, banks are required by Law Number 10 of 1998 and OJK Regulation Number 11/POJK.03/2022 to protect consumer data. For risk reduction and data and service recovery after a cyberattack, digital banks must establish a Disaster Recovery Center (DRC) and Disaster Recovery Plan (DRP). This study also highlights the importance of banks taking preventive and corrective actions to protect customers of digital banking services, as well as the responsibility of banks to comply with legislative requirements to protect the security of their customers' data.
Keywords: *Banking Law, Digital Era, Banks*

ABSTRAK

Penelitian ini bermaksud untuk mengevaluasi tanggung jawab hukum bank untuk melindungi nasabah yang menggunakan layanan perbankan digital. Di lain sisi, kasus perbankan digital di Indonesia akan diperiksa, dengan penekanan pada tindakan yang bisa diimplementasikan untuk meningkatkan keamanan sistem. Pendekatan penelitian kepustakaan, yang bergantung pada pencarian data sekunder atau bahan pustaka, digunakan dalam studi ini. Dalam hal ini, bank diharuskan oleh Undang-Undang Nomor 10 Tahun 1998 dan Peraturan OJK Nomor 11/POJK.03/2022 untuk melindungi data konsumen. Untuk pengurangan risiko dan pemulihan data dan layanan pasca-serangan siber, bank digital harus membangun Pusat Pemulihan Bencana (DRC) dan Rencana Pemulihan Bencana (DRP). Penelitian ini juga menyoroti betapa pentingnya bagi bank untuk mengambil tindakan pencegahan dan perbaikan untuk melindungi nasabah layanan perbankan digital, serta tanggung jawab bank untuk mematuhi persyaratan legislatif guna melindungi keamanan data nasabah mereka.
Kata Kunci: Hukum Perbankan, Era Digital, Bank

Article History
Received: Desember 2024
Reviewed: Desember 2024
Published: Desember 2024

Plagirism Checker No 234
Prefix DOI : Prefix DOI :
10.8734/CAUSA.v1i2.365
Copyright : Author
Publish by : CAUSA

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

INTRODUCTION

Bank sangat penting dalam ekonomi modern sebab berfungsi sebagai sumber pendanaan yang vital dan memfasilitasi aktivitas ekonomi. Bank bertindak sebagai jembatan antara individu yang memiliki kelebihan dana dan individu yang membutuhkan dana. Hal ini memungkinkan masyarakat untuk mengakses dana melalui pinjaman dan investasi. Operasi bank diatur oleh sejumlah undang-undang dan peraturan untuk melindungi kepentingan keuangan dan hubungan kontraktual. Di Indonesia, dasar hukum perbankan diatur dalam Undang-Undang

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 8 No 4 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

No. 10 tahun 1998 tentang Perbankan amandemen dari Undang-Undang No. 7 tahun 1992 yang memuat definisi, fungsi, dan pengawasan bank.

Di era globalisasi yang semakin berkembang, penggunaan bank digital di Indonesia terus meningkat, menjadikannya pilihan utama bagi banyak masyarakat. Hal ini disebabkan oleh tingkat kepraktisan yang ditawarkan, di mana sejumlah layanan perbankan, seperti transfer dana, pembayaran tagihan, hingga pengelolaan keuangan, bisa dilakukan dengan mudah melalui perangkat digital seperti ponsel pintar atau komputer. Bank digital juga memberikan efisiensi yang tinggi, memungkinkan nasabah untuk mengakses layanan kapan saja dan di mana saja tanpa harus melakukan kunjungan ke kantor cabang fisik. Dengan sejumlah keunggulan itu, tidak mengherankan jika bank digital semakin diminati sebagai solusi perbankan modern.

Tetapi, tingkat keamanan dalam penggunaan layanan perbankan di era digital sering kali dianggap masih rendah, terutama mengingat tingginya risiko peretasan data pribadi nasabah yang dilakukan oleh sejumlah pihak yang tidak bertanggung jawab. Informasi sensitif nasabah seperti nomor rekening, data identitas, hingga riwayat transaksi banyak digunakan oleh sejumlah kasus kebocoran data dan serangan siber yang akhirnya dimanfaatkan untuk kejahatan. Salah satu kasusnya, yaitu peretasan Bank Syariah Indonesia yang diretas oleh serangan ransomware dari sekelompok hacker yang menyebabkan kebocoran data sensitif nasabah.

Awalnya, BSI mengklaim gangguan layanan disebabkan oleh pemeliharaan sistem. Tetapi, pada 14 Mei 2023, terungkap bahwa gangguan itu akibat serangan ransomware dari kelompok peretas Lock Bit, yang mengenkripsi data dan meminta tebusan. Mereka memberikan batas waktu 72 jam pada BSI dan mengancam merusak reputasi bank jika permintaan tidak dipenuhi. Meskipun manajemen BSI tetap menyebutkan alasan pemeliharaan, peretas akhirnya berhasil menyandera data nasabah. Hal ini menjadi salah satu contoh nyata dari kompleksitas ancaman keamanan siber di sektor perbankan.

Berdasarkan uraian di atas, maka permasalahan yang perlu diteliti adalah bagaimana implementasi layanan perbankan digital di Indonesia dan bagaimana bank secara hukum diwajibkan untuk melindungi dan menjamin keamanan nasabah atas implementasi layanan perbankan digital dalam hal terjadi serangan siber pada Bank Syariah Indonesia.

Mengetahui bagaimana layanan perbankan digital diimplementasikan di Indonesia dan bagaimana melindungi nasabah yang menggunakan layanan itu apabila terjadi serangan siber pada Bank Syariah Indonesia merupakan dua tujuan utama dari penelitian ini, yang merefleksikan permasalahan yang diangkat dalam penulisan itu di atas.

Karya Nur Kholis, yang berfokus pada perbankan yang memanfaatkan kemajuan era digital (Kholis, 2018), Asti Marlina & Widhi Ariyo Bimo yang mengkaji bagaimana bank bisa meningkatkan kepuasan nasabah melalui digitalisasi (Marlina, Asti., & Bimo, 2018), Talumewo yang mengkaji pertanggungjawaban bank dalam upaya melindungi nasabah dari tindak pidana ITE (Talumewo, 2013), dan Mbama & Catejan yang meneliti mengenai pengalaman nasabah dalam implementasi teknologi perbankan digital di Inggris (Mbama., 2018).

Meskipun pengembangan layanan perbankan ke era digital merupakan topik yang dibahas dalam studi ini dan penelitian sebelumnya, penelitian saat ini berfokus pada perlindungan konsumen yang menggunakan layanan perbankan digital dan mengkaji kasus perbankan digital Indonesia dan tindakan yang bisa diambil dengan tujuan agar keamanan sistem dengan studi kasus Bank Syariah Indonesia bisa diperkuat.

RESEARCH METHOD

Library research adalah jenis penelitian yang diimplementasikan dalam studi ini. Data sekunder atau sumber pustaka digunakan untuk melakukan penelitian ini. Dalam penelitian ini, metode yang digunakan adalah studi pustaka, yakni dengan meneliti sumber pustaka berupa buku, jurnal, dan karya tulis terdahulu yang membahas masalah yang diteliti. Hukum yuridis normatif adalah metode penelitian yang diimplementasikan dalam studi ini. Di mana penelitian ini berfokus untuk mengkaji Kewajiban Hukum Perbankan di Indonesia dalam Menjamin Keamanan Transaksi dan Nasabah di Era Digital.

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 8 No 4 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

FINDINGS AND DISCUSSION

Peraturan Perbankan Digital

Peraturan OJK No. 12/POJK.03/2018 menyatakan bahwa kualitas layanan nasabah akan ditingkatkan oleh banyak bank saat terjadi persaingan yang kompetitif di sektor perbankan Indonesia dengan cara yang lebih efektif dan efisien. Kemampuan bank harus senantiasa ditingkatkan dengan mengoordinasikan strategi bisnis yang lebih terfokus untuk mencapai efektivitas dan efisiensi ini (Dhendana, 2013).

Inovasi dalam layanan perbankan bisa didukung dengan adanya pemanfaatan teknologi informasi secara efisien. Inovasi layanan yang didukung teknologi informasi serta implementasi strategi yang tepat mendorong bank untuk memasuki era layanan keuangan digital.

Automated Teller Machines (ATMs), *Cash Deposit Machines* (CDMs), *Point of Sale* (POS), *Electronic Data Capture* (EDC), *Telephone Banking*, *SMS Banking*, *Internet Banking*, *dan Mobile Banking* merupakan contoh saluran distribusi layanan perbankan elektronik selaras dengan apa yang didefinisikan oleh Peraturan OJK No. 12/POJK.03/2018. Layanan perbankan digital dijelaskan sebagai aktivitas operasional atau layanan perbankan yang bisa dilakukan secara mandiri dan memanfaatkan sumber daya elektronik atau digital yang dimiliki oleh bank ataupun media digital yang dimiliki oleh nasabah atau calon nasabah bank.

Registrasi, komunikasi, akses informasi, pembukaan rekening, aktivitas perbankan, dan penutupan rekening adalah sejumlah hal yang bisa dilakukan oleh pengguna dengan menggunakan layanan itu. Di lain sisi, layanan ini juga memuat informasi yang tidak terkait dengan produk perbankan, seperti investasi, nasihat keuangan, transaksi melalui sistem perdagangan elektronik, dan kebutuhan lainnya. (Tarigan & Paulus, 2019)

Salah satu pengembangan layanan perbankan elektronik yang ditujukan untuk memberikan efisiensi dan kenyamanan bagi konsumen adalah implementasi layanan perbankan digital. Tetapi, selaras dengan apa yang diuraikan dalam Pasal 18 Peraturan OJK No. 12/POJK.03/2018, implementasinya harus mengikuti standar khusus. Memiliki peringkat profil risiko 1 atau 2 berdasarkan penilaian tingkat kesehatan bank yang terakhir adalah salah satu persyaratan utama.

Pasal 24 POJK Nomor 12/POJK.03/2021 memaparkan bahwa rencana bisnis untuk beralih ke perbankan digital harus menggabungkan teknologi mutakhir dan aman untuk memenuhi aspirasi konsumen. Di lain sisi, menurut POJK, perbankan digital perlu memiliki manajemen risiko yang memadai dan mampu menerapkan model bisnis perbankan yang layak dan beretika. Penerapan perbankan digital memerlukan tata kelola sebagai landasan kepatutan, yang mencakup perekrutan direktur dengan pengalaman teknologi informasi.. Melindungi keamanan data konsumen dan bisa mendukung upaya yang memajukan pertumbuhan ekosistem keuangan digital dan/atau inklusi keuangan merupakan prasyarat tambahan untuk implementasi bank digital.

Di lain sisi, manajemen dan infrastruktur teknologi informasi harus dimiliki oleh bank yang menawarkan layanan perbankan digital. Berdasarkan aktivitas usaha, bank juga harus menjadi bagian dari kelompok bank umum yang setidaknya bisa menyediakan layanan perbankan elektronik selaras dengan peraturan OJK.

Di negara-negara industri di Asia, layanan perbankan digital semakin populer. Sejumlah bank sudah mulai menawarkan layanan perbankan digital di kawasan ini, yang memiliki potensi yang sangat besar. Bank DBS Singapura adalah salah satunya; pada tahun 2016, bank ini meluncurkan produk Digibank di India. Kemudian, pada tahun 2017, layanan perbankan digital khusus ponsel ini diperluas ke Indonesia. Di lain sisi, KakaoBank, sebuah layanan perbankan digital di Korea Selatan, sudah berkembang dengan pesat. KakaoBank merupakan salah satu layanan perbankan digital teratas di Asia, dengan 5,5 juta nasabah.

Tak terkecuali di Indonesia, kini marak sekali Bank Digital yang digunakan oleh masyarakat Indonesia untuk menunjang kebutuhan dan keperluan sehari-hari. Masyarakat Indonesia bisa memilih bank digital yang paling selaras dengan kebutuhan mereka sebab ada begitu banyak kemungkinan yang bisa diakses. Sebagai contoh ada Bank Jenius, Seabank, Line

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 8 No 4 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

Bank, BCA Blu, dan lain sebagainya. Tak hanya itu, Bank-bank di Indonesia juga berlomba-lomba dalam menciptakan transaksi digital yang efektif dan efesien, yakni M-Banking BCA, Livin by Mandiri, M-Banking BSI, dan lain sebagainya. (Faried Wijaya dan Soetatwo Hadiwigeno, 1999)

Banyaknya layanan perbankan digital sangat memudahkan masyarkat, tetapi di balik sisi positif yang ada, tentunya dalam penggunaan sarana perbankan digital adapula sisi negatifnya. Seperti rentannya kebocoran data, saldo rekening yang tiba-tiba hilang, dan juga keamanan nasabah itu sendiri dalam menggunakan perbankan digital.

Pasal 24 huruf (e) POJK Nomor 12/POJK.03/2021 memaparkan bahwa implementasi bank digital harus memastikan keamanan data nasabah, yang saat ini menjadi hambatan hukum paling signifikan yang dihadapi perbankan digital. Mengingat masih banyak yang menyalahgunakan data nasabah perbankan, keamanan data menjadi perhatian penting bagi sektor digital saat ini.

Keamanan dan perlindungan data konsumen menjadi perhatian utama perbankan digital saat ini karena terkait dengan kepercayaan konsumen, kesehatan perbankan, dan fungsi perantara perbankan. Sehubungana dengan hal itu, rancangan undang-undang (RUU) perlindungan data pribadi harus segera disahkan oleh pemerintah untuk memastikan keamanan dan keselamatan data nasabah sebaik mungkin dalam implementasi bank digital. (Dr. Rio Christiawan, S.H., M.Hum., 2021)

Keamanan dan Perlindungan Konsumen pada Bank Digital

Perlindungan preventif dan perlindungan represif adalah dua strategi utama untuk melindungi nasabah saat layanan keuangan digital diimplementasikan. Tujuan dari perlindungan preventif adalah untuk menghindari atau meramalkan potensi kejadian yang tidak diinginkan yang akan terjadi pada nasabah di masa depan. Untuk mengurangi bahaya bagi konsumen, upaya ini dilakukan dengan berkonsultasi dengan peraturan dan regulasi yang relevan. (Candrawati, 2014)

Di lain sisi, perlindungan represif digunakan saat klien mengalami kerugian akibat kejadian yang tidak diinginkan. Melalui upaya penyelesaian selaras dengan batasan hukum yang relevan, perlindungan ini berusaha untuk mengatasi masalah atau konflik yang muncul. Diharapkan bahwa kedua strategi ini akan memberikan rasa keadilan dan keamanan bagi pengguna layanan keuangan digital. (Jahri, 2016)

A. Perlindungan dari Tindakan Preventif bagi Nasabah yang Menggunakan Layanan Perbankan Online

Undang-Undang No. 10 Tahun 1998 tentang Perbankan, Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen, dan Peraturan OJK No. 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum adalah sejumlah regulasi yang mengatur perlindungan preventif bagi nasabah perbankan. Perlindungan hukum yang ditawarkan oleh bank terkait layanan perbankan digital memuat sejumlah aspek penting berikut:

1. Penyediaan informasi tentang potensi ancaman kerugian bagi nasabah. Transparansi terkait potensi risiko yang berhubungan dengan layanan keuangan digital wajib diberikan oleh bank. Hal ini bermaksud untuk menjamin bahwa nasabah memiliki akses pada informasi mengenai operasional dan kondisi bank, sekaligus mendorong keterbukaan dalam industri perbankan.
2. Kerahasiaan bank. Bank bisa mempertahankan kepercayaan publik dengan memastikan bahwa informasi pribadi nasabah, seperti data tabungan dan status keuangan, tidak disalahgunakan. Perlindungan pada kerahasiaan merupakan landasan utama kepercayaan konsumen pada layanan keuangan digital.
3. Jaminan dana nasabah. Semua bank diwajibkan menjamin dana nasabah yang menggunakan layanan perbankan digital. Lembaga Penjamin Simpanan (LPS) didirikan untuk menjalankan jaminan ini, sehingga melindungi dana nasabah dalam situasi yang merugikan. (Rani, 2017)

Di lain sisi, UU Perlindungan Konsumen juga menjabarkan upaya pemerintah yang dilakukan dengan maksud agar nasabah perbankan bisa dilindungi secara umum. Tanggung jawab UU Perlindungan Konsumen untuk melindungi konsumen pengguna layanan perbankan digital wajib dipenuhi oleh bank. Berikut adalah sejumlah kewajiban yang harus dilakukan oleh bank sebagai suatu badan usaha:

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 8 No 4 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

a. Beritikad baik dalam menjalankan aktivitas usaha seperti menyediakan layanan perbankan digital.
b. Memberikan jaminan mutu atas produk dan layanan seperti layanan perbankan digital, yang diiklankan pada masyarakat umum selaras dengan standar mutu.
c. Menyampaikan informasi secara jelas, akurat, dan jujur tentang status jaminan atas produk atau layanan. Bank wajib memberikan penjelasan tentang penggunaan, pemeliharaan, dan perbaikan sebagai pelaku usaha.
d. Bank wajib mengganti kerugian yang timbul akibat penggunaan produk atau layanan selaras dengan perjanjian.

B. Perlindungan dari Tindakan Represif bagi Nasabah yang Menggunakan Layanan Perbankan Online

Hak-hak konsumen bisa dilindungi dengan cara menangani apa saja yang menjadi keluhan mereka (Panjaitan, 2012). Jika keluhan konsumen tidak ditangani secara efisien, bank pada akhirnya akan menghadapi risiko reputasi yang lebih besar yang bisa merusak kepercayaan publik.

Peraturan BI No. 10/10/PBI/2008, yang mengubah Peraturan BI No. 7/7/PBI/2005, yang mengatur tentang penyelesaian pengaduan nasabah memaparkan bahwa "*pengaduan adalah pernyataan ketidakpuasan nasabah yang disebabkan oleh potensi kerugian finansial bagi nasabah yang diduga akibat kesalahan atau kelalaian bank*." Berdasarkan peraturan ini, bank harus mengikuti proses formal untuk menangani semua pengaduan yang dibuat oleh nasabah atau perwakilan nasabah. Proses ini harus memuat penerimaan pengaduan, penanganan dan penyelesaiannya, serta pemantauan bagaimana pengaduan ditangani dan diselesaikan.

Surat Edaran OJK No. 2/SEOJK.07/2014 tentang Pelayanan dan Penyelesaian Pengaduan Konsumen pada Pelaku Usaha Jasa Keuangan juga mengatur tata cara penanganan pengaduan konsumen. Berdasarkan ketentuan itu, bank wajib memberikan ganti rugi (Remedies) dan pernyataan permintaan maaf apabila menangani pengaduan nasabah yang mengalami kerugian secara materiil.

Pada kenyataannya, upaya bank dalam melindungi konsumen layanan perbankan digital sebagai penyedia jasa merupakan salah satu bentuk pertanggungjawaban pada nasabah yang mengalami kerugian (Talumewo, 2013). Selaras dengan Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, dan Peraturan OJK No. 12/POJK.03/2018, kewajiban ini bermaksud untuk melindungi kepentingan nasabah. Di lain sisi, untuk menjaga kepercayaan masyarakat pada bank yang menyelenggarakan layanan perbankan digital, kewajiban ini juga bermaksud untuk menekan kemungkinan risiko penurunan reputasi bank dalam jangka panjang.

Kasus Serangan Siber pada M-Banking Bank Syariah Indonesia dan Kewajiban Perbankan dalam Perlindungan Nasabah

Di era digital pada masa kini, kebocoran data adalah masalah yang signifikan di banyak industri termasuk perbankan, seperti yang terjadi pada BSI akhir-akhir ini. Meskipun masalah kebocoran data pribadi bukanlah hal yang baru, tetapi hal ini merupakan masalah yang serius dan mengkhawatirkan. (Azarine, 2024) Nasabah dan bank mengalami kerugian yang signifikan akibat gangguan sistem yang menyebabkan nasabah BSI tidak bisa menggunakan ATM, mobile banking, atau penarikan uang tunai selama sekitar seminggu. Lebih jauh lagi, sebab kepercayaan publik pada bank menurun akibat kebocoran data nasabah, situasi memburuk. Di luar dampak yang sudah dirasakan nasabah, hal ini bisa mengakibatkan peningkatan kerugian bank. (Integra Teknologi Solusi, 2023)

Hal ini bisa menjadi bencana jika informasi pribadi konsumen, seperti nomor rekening, nomor kartu kredit, informasi identitas, dan rincian keuangan, terungkap. Serangan siber, kelalaian keamanan perusahaan, atau manajemen data yang ceroboh, semuanya bisa mengakibatkan pengungkapan itu. Kebocoran data perbankan pribadi bisa membahayakan kepercayaan konsumen pada lembaga keuangan dan secara serius merusak reputasi mereka

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 8 No 4 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

selain meningkatkan bahaya pencurian identitas, penipuan, dan penyalahgunaan keuangan. (Azarine, 2024)

Menurut standar perbankan, informasi pribadi nasabah sangatlah berharga dan perlu dilindungi dengan baik. Nasabah harus memberikan informasi pribadi untuk bisa menggunakan layanan transaksi elektronik. Hal ini diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 26 ayat (1), yang mengatur bahwa persetujuan dari yang bersangkutan harus diperoleh sebelum menggunakan informasi mengenai data pribadinya. Akan tetapi, tingkat perlindungan data pribadi yang ada pada sistem keamanan perbankan masih belum memadai.

Undang-Undang Nomor 19 Tahun 2016 di Indonesia mengubah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tentang perlindungan data pribadi. Tindak pidana yang memengaruhi privasi dan informasi pribadi, serta ketentuan tentang sanksi hukum atas pencurian data bisa ditangani dengan adanya sejumlah landasan hukum yang ditetapkan dalam undang-undang ini. Ketentuan pidana UU ITE yang berkaitan dengan pencurian data diuraikan dalam Pasal 30-35, sementara pasal lainnya mengatur sejumlah pelanggaran. Tindak pidana yang diancam dengan pidana denda paling banyak Rp 600.000.000,00 sampai dengan Rp 800.000.000,00 dan pidana penjara paling lama 6 tahun adalah perbuatan menggunakan sistem elektronik untuk memperoleh data atau dokumen. (Idris Balaka и съавт., 2024)

Melalui Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum yang mulai berlaku sejak 7 Oktober 2022, bank wajib memiliki *Disaster Recovery Center* dalam rangka memitigasi risiko teknologi. Data, informasi, dan fungsi sistem elektronik penting yang terganggu atau rusak akibat bencana alam ataupun bencana yang disebabkan oleh manusia bisa dipulihkan dengan memanfaatkan fasilitas ini. Agar bank bisa tetap menjalankan aktivitas usahanya secara esensial saat terjadi gangguan atau bencana, maka bank juga harus memiliki *Disaster Recovery Plan*, yaitu dokumen yang merinci strategi dan prosedur penggantian dan/atau pemulihan akses pada data, perangkat keras, dan perangkat lunak. (Nisaputra, 2023)

Berkaitan dengan hal itu data-data nasabah wajib dilindungi oleh bank sebagaimana Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur hal ini, dengan menegaskan bahwa semua bank wajib menjaga kerahasiaan informasi nasabahnya. Pasal 40 Undang-Undang Perbankan memaparkan bahwa informasi yang berkaitan dengan nasabah wajib dirahasiakan dan tidak boleh diungkapkan pada pihak ketiga tanpa persetujuan nasabah kecuali dalam keadaan khusus yang diatur dalam peraturan perundang-undangan.

Sejumlah hal yang bisa dilakukan untuk memperkuat keamanan nasabah baik oleh Bank Syariah Indonesia ataupun bank digital lainnya selaras dengan Peraturan OJK No. 11/POJK.03/2022, bank wajib memiliki *Disaster Recovery Center* (DRC) *dan Disaster Recovery Plan* (DRP) untuk pemulihan data dan layanan pasca-serangan. Di lain sisi, BSI harus memperkuat proteksi data pribadi nasabah dengan enkripsi yang lebih ketat dan kontrol akses yang jelas, serta mematuhi Undang-Undang Perlindungan Data Pribadi. Bank juga harus memastikan kepatuhan pada Undang-Undang Perbankan dan Undang-Undang Perlindungan Konsumen, dengan memberikan informasi transparan tentang risiko layanan digital dan mengedukasi nasabah tentang pentingnya menjaga keamanan akun pribadi mereka.

CONCLUSION

Dengan implementasi teknologi informasi yang efektif dan undang-undang yang mendukung seperti Peraturan OJK No.12/POJK.03/2018, layanan perbankan digital di Indonesia semakin berkembang. Peraturan ini menjamin bahwa bank digital harus mematuhi persyaratan khusus untuk manajemen risiko, perlindungan data, dan tata kelola yang tepat.

Upaya preventif dan represif digunakan untuk melindungi konsumen yang menggunakan layanan perbankan digital. Langkah-langkah preventif, seperti melindungi kerahasiaan data dan membuat informasi risiko menjadi transparan, sangat penting untuk menghindari kerugian bagi klien. Di lain sisi, perlindungan represif diimplementasikan dengan menanggapi keluhan konsumen dan menawarkan penggantian kerugian jika kerugian terjadi akibat kesalahan bank.

Tetapi, kebocoran informasi pribadi merupakan masalah signifikan pada layanan perbankan digital yang bisa merusak citra bank dan merusak kepercayaan konsumen, sehingga memerlukan perlindungan keamanan data yang lebih kuat dan menyeluruh.

REFERENCES

Azarine, A. M. (2024). Bank BSI Pasca Serangan Siber: Mengungkap Potensi Kompensasi Bagi Nasabah. *LK2FHUI*. https://lk2fhui.law.ui.ac.id/portfolio/bank-bsi-pasca-serangan-siber-mengungkap-potensi-kompensasi-bagi-nasabah/

Candrawati, N. N. A. (2014). Perlindungan Hukum Terhadap Pemegang Kartu E-Money Sebagai Alat Pembayaran Dalam Transaksi Komersial. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *3*(1).

Dhendana, T. (2013). Penerapan Prudential Banking Principle dalam Upaya Perlindungan Hukum Bagi Nasabah Penyimpan Dana. *Lex et Societatis*, *1*(1).

Dr. Rio Christiawan, S.H., M.Hum., M. K. (2021). *Tantangan Hukum Bank Digital*. HukumOnline.com. https://www.hukumonline.com/berita/a/tantangan-hukum-bank-digital-lt61308a5a9a319/?page=3

Faried Wijaya dan Soetatwo Hadiwigeno. (1999). Lembaga-Lembaga Keuangan dan Bank. B *Buku Ajar*.

Idris Balaka, K., Rahman Hakim, A., & Dwi Sulistyany, F. (2024). Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital. *Yustitiabelen*, *10*(2), 105–130. https://doi.org/10.36563/yustitiabelen.v10i2.1167

Integra Teknologi Solusi. (2023). *Kasus Sistem BSI Down: Pelajaran yang Bisa Diambil*. IntegraSolusi. https://integrasolusi.com/blog/kasus-sistem-bsi-down-pelajaran-yang-bisa-diambil/

Jahri, A. (2016). Perlindungan Nasabah Debitur Terhadap Perjanjian Baku Yang Mengandung Klausula Eksonerasi Pada Bank Umum Di Bandar Lampung. *Fiat Justisia Journal of Law*, *10*(2).

Kholis, N. (2018). Perbankan Dalam Era Baru Digital. *Jurnal Economicus*, *9*(1).

Marlina, Asti., & Bimo, W. A. (2018). Digitalisasasi Bank Terhadap Peningkatan Pelayanan Dan Kepuasan Nasabah Bank. *Jurnal Ilmiah Inovator*, *Edisi Maret*, 14–33.

Mbama., & C. (2018). Digital banking, customer experience and bank financial performance : UK customers' perceptions. *International Journal of Bank Marketing*, *36*(2), 230–235.

Nisaputra, R. (2023). *Belajar dari Kasus Bank Syariah Indonesia (BSI)*. Info Bank News. https://infobanknews.com/belajar-dari-kasus-bank-syariah-indonesia-bsi/

Panjaitan, L. (2012). Analisis Penanganan Carding dan Perlindungan Nasabah dalam kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008. *Incomtech Jurnal Telekomunikasi dan kompute*, *3*(1).

Rani, M. (2017). Perlindungan Otoritas Jasa keuangan Terhadap kerahasiaan dan keamanan data pribadi Nasabah Bank. *Jurnal Sela*, *2*(1).

Talumewo, F. (2013). Pertanggungjawaban Bank Terhadap Nasabah Yang Menjadi Korban Kejahatan Informasi Dan Transaksi Elektronik. *Jurnal Lex Crime*, *2*(1), 132–147.

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indonesia*, *1*(3), 294–307. https://doi.org/10.14710/jphi.v1i3.294-307