

ANALISIS TANGGUNG JAWAB BANK DALAM PERLINDUNGAN DATA NASABAH: STUDI KASUS
PERBANKAN KONVENSIONAL DAN PERBANKAN DIGITAL

Annisa Calista Maharani, Fakultas Hukum Universitas Udayana,
e-mail: annisacalistamhr@gmail.com

I Wayan Novy Purwanto, Dosen Fakultas Hukum Universitas Udayama,
e-mail: novy_purwanto@gmail.com

ABSTRAK

Perlindungan data pribadi menjadi isu penting dalam era digitalisasi saat ini, terutama dalam penggunaan teknologi informasi oleh bank menimbulkan risiko terhadap keamanan data pribadi nasabah. Studi ini menggunakan metode penelitian normatif untuk menganalisis peraturan hukum yang mengatur perlindungan data pribadi di Indonesia, serta memeriksa implementasi dan kepatuhan bank terhadap regulasi tersebut. Hasil analisis menunjukkan bahwa bank memiliki kewajiban hukum yang jelas untuk melindungi data nasabah sesuai dengan Undang-Undang Perlindungan Data Pribadi dan regulasi terkait lainnya. Bank konvensional cenderung mengikuti pendekatan yang lebih tradisional dengan kebijakan internal yang mapan, sedangkan bank digital dihadapkan pada tantangan unik dalam menghadapi perkembangan teknologi dan regulasi yang cepat berubah. Penelitian ini juga mengidentifikasi beberapa isu hukum yang muncul dalam implementasi kebijakan perlindungan data di kedua jenis bank tersebut, seperti transparansi, hak privasi, dan tanggung jawab dalam kasus pelanggaran data, termasuk beberapa kasus yang terjadi berkenaan dengan hal tersebut sehingga perlindungan data nasabah oleh bank memerlukan pendekatan hukum yang holistik dan penegakan yang ketat untuk memastikan kepatuhan yang efektif terhadap hukum yang berlaku.

Kata Kunci: Hukum Perbankan, Perlindungan Data Pribadi, Bank Digital, Bank Konvensional

ABSTRACT

Data protection has become a critical issue in the current digital era, where banks' use of information technology poses risks to the security of customers' personal data. This study employs a normative legal research method to analyze the legal regulations governing data protection in Indonesia and examines banks' implementation and compliance with these regulations. The analysis shows that banks have clear legal obligations to protect customer data under the Personal Data Protection Act and other relevant regulations. Conventional banks tend to follow a more traditional approach with established internal policies, while digital banks face unique challenges in coping with rapid technological advancements and evolving regulations. The study also identifies several legal issues arising in the implementation of data protection policies in both types of banks, such as transparency, privacy rights, and liability in case of data breaches. In conclusion, safeguarding customer data by banks requires a holistic legal approach and rigorous enforcement to ensure effective compliance with applicable laws.

Keywords: Banking Law, Personal Data Protection, Digital Bank, Conventional Bank

Article history

Received: November 2025

Reviewed: November 2025

Published: November 2025

Plagiarism checker no 473

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](https://creativecommons.org/licenses/by-nc/4.0/)

I. Pendahuluan

1.1 Latar Belakang Masalah

Perbankan merupakan lembaga keuangan yang memegang peran strategis dalam mendukung pertumbuhan perekonomian suatu negara¹. Lembaga tersebut memiliki dua fungsi utama yaitu untuk menghimpun dan menyalurkan dana masyarakat. Dalam menjalankan fungsinya, bank sendiri dibedakan menjadi dua jenis yaitu bank konvensional dan bank syariah. Berdasarkan Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah (yang sekarang telah diubah dengan Undang-Undang Nomor 4 Tahun 2023 tentang Penguatan Sektor Keuangan), bank konvensional diartikan sebagai bank yang menjalankan kegiatan usaha secara konvensional dan terbagi atas bank umum konvensional dan bank perekonomian rakyat. Adapun bank syariah didefinisikan sebagai Badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan maupun investasi, kemudian menyalurkannya kembali melalui pembiayaan atau mekanisme lain yang berlandaskan prinsip syariah. Jenis badan usaha ini mencakup bank umum syariah dan bank perekonomian rakyat syariah². Meskipun terdapat perbedaan prinsip antara kedua jenis bank tersebut, umumnya layanan yang diberikan oleh bank berupa pinjaman kredit, simpanan tabungan, jasa mengirimkan uang atau transfer, dan berbagai macam jasa lainnya yang berkaitan dengan uang.

Seiring dengan perkembangan zaman, layanan perbankan juga ikut berkembang dengan memanfaatkan Teknologi Informasi yang saat ini dikenal sebagai Financial Technology atau yang biasa disingkat sebagai Fintech. Adanya digitalisasi dalam sistem perbankan sesungguhnya bukan merupakan sebuah pilihan melainkan sebuah keharusan demi meningkatkan kenyamanan dan efisiensi dalam pelayanan setiap nasabah. Adanya pemanfaatan teknologi ini mendorong perbankan kepada era baru yakni era perbankan digital. Peraturan OJK No. 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum menyebutkan bahwa layanan perbankan digital merupakan layanan elektronik yang dikembangkan dengan mengoptimalkan data nasabah untuk memberikan pelayanan yang lebih cepat, mudah, dan sesuai kebutuhan (customer experience). Melalui layanan ini, nasabah maupun calon nasabah dapat secara mandiri mengakses informasi, berkomunikasi, melakukan registrasi, membuka dan menutup rekening, serta melakukan berbagai transaksi perbankan dengan tetap memperhatikan aspek keamanan. Selain itu, layanan tersebut juga memungkinkan akses terhadap informasi dan transaksi di luar produk perbankan, seperti layanan keuangan (financial advisory), investasi, transaksi e-commerce, dan layanan lainnya tanpa harus datang langsung ke kantor bank³. Dalam konteks ini, bank digital dapat menjalankan kegiatan usahanya sepenuhnya melalui media elektronik tanpa kehadiran kantor fisik selain kantor pusat, atau dengan penggunaan kantor fisik yang sangat terbatas.

Pengembangan tersebut tentu membawa keuntungan bagi kedua belah pihak, baik bagi bank maupun bagi nasabah. Bagi pihak bank digital tidak perlu mengeluarkan modal lebih untuk membuka kantor cabang seperti bank pada umumnya dan dapat menghubungi nasabah secara lebih efisien melalui media digital tersebut. Selanjutnya, pihak nasabah sendiri tidak perlu mengeluarkan energinya untuk pergi ke bank secara fisik dan dapat memperoleh kebutuhannya secara lebih efektif dan efisien dimanapun ia berada⁴. Namun, diantara keuntungan tersebut terdapat resiko yang perlu diwaspadai

¹ Usanti, Trisandini dan Abd. Shomad. (2016). Hukum Perbankan. Prenamedia Group: Jakarta, hlm. 1

² *Ibid.*

³ Tarigan, Herdian Ayu dkk. (2019). Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. Jurnal Pembangunan Hukum Indonesia, 1(3), hlm. 296

⁴ Usanti, Trisandini dan Abd. Shomad, op. cit. hlm. 15

sehingga perlu dipikirkan upaya preventif maupun represif untuk mengatasi resiko yang akan muncul. Beberapa permasalahan yang dapat muncul misalnya seperti gangguan pada sistem, pencurian sampai penyalahgunaan data nasabah, maupun pencurian dana secara tidak sah yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Oleh sebab itu, pihak bank memerlukan infrastruktur sistem dan media digital yang memadai sebelum membuka layanan digital kepada pihak nasabah demi mencegah terjadinya permasalahan tersebut. Perlindungan data nasabah harus dibuat dengan sistem sekuritas tinggi agar tidak adanya lagi masalah peretasan maupun penyalahgunaan data pribadi milik nasabah.

Merujuk kepada hal tersebut, sebetulnya pihak nasabah sebagai konsumen hak-haknya telah dilindungi oleh Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK). UUPK merupakan perangkat hukum yang menyediakan pedoman yang pasti untuk melindungi hak dan kepentingan nasabah sebagai konsumen. Konsumen berhak mendapatkan ganti rugi apabila pihak pelaku usaha melakukan pelanggaran atau merugikan konsumen itu sendiri. Selain itu, konsumen berhak memperoleh informasi yang akurat, sehingga bank wajib memberikan penjelasan secara jujur dan terbuka kepada nasabah apabila terjadi kendala pada layanan digital⁵. Selain UUPK, tersedia pula ketentuan perundang-undangan lain yang menjamin perlindungan hak nasabah yaitu dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. dalam aturan hukum tersebut diatur secara lebih rinci terutama mengenai penyelesaian sengketa maupun ancaman pidana apabila terdapat pelanggaran berkaitan dengan data pribadi.

Pada kenyataannya, meski sudah terdapat peraturan perundang-undangan yang berlaku, pelaku kejahatan siber masih terus berkeliaran dan masih marak terjadi di sekitar kita sehingga mengganggu kenyamanan nasabah untuk melakukan kegiatan dalam ranah perbankan. Misalnya saja Kasus kebocoran data nasabah PT Bank Syariah Indonesia Tbk (BSI) pada awal Mei tahun lalu menimbulkan kerugian yang signifikan baik bagi nasabah maupun pihak bank. Kemudian diketahui bahwa insiden tersebut disebabkan oleh aksi peretasan yang dilakukan oleh kelompok hacker LockBit, yang diduga telah mengunggah dan memperjualbelikan data nasabah BSI di pasar gelap⁶. Tidak hanya pihak eksternal, permasalahan risiko pelayanan digital juga dapat muncul dari pihak internal itu sendiri. Dikutip dari Merdeka.com yang terbit tanggal 17 Februari 2020 dengan judul “Mafia Jual Beli Data Pribadi”, Lana seorang pegawai bank membagikan ceritanya yang hanya bermodalkan ratusan ribu, ia bisa mendapatkan ribuan data pribadi. Lana menjelaskan bahwa dia dapat membeli data pribadi dari temannya yang juga bekerja di bank lain dengan kisaran harga sekitar 200 ribu hingga 500 ribu rupiah. Semakin lengkap suatu data maka harga jual akan semakin mahal. Lana juga menjelaskan bahwa sudah menjadi rahasia umum antar bank kerap saling memperjualbelikan data calon nasabah maupun data nasabah yang sudah ada. Akibatnya, tidak jarang nasabah yang telah memiliki kartu kredit di satu bank menerima berbagai penawaran melalui telepon atau SMS untuk membuat kartu kredit dari bank lain. Menurut Lana, tidak jarang oknum pegawai bank memanfaatkan jabatannya untuk mendapatkan keuntungan sendiri, bahkan ada yang sampai menjual data nasabah kepada penjahat pembobol rekening. Berdasarkan permasalahan yang diangkat oleh Merdeka.com ini, dapat diketahui bahwa sistem keamanan perbankan terutama pelaksanaan perlindungan data pribadi di Indonesia masih belum berjalan secara optimal sehingga penulis tertarik untuk meneliti permasalahan ini secara lebih lanjut.

⁵ Marcelliana, Vanesha dkk. (2023). Penerapan Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia dalam Kasus Kebocoran Data Nasabah. Jurnal Publikasi Ilmu Hukum, 1(2), hlm. 182

⁶ Marcelliana, Vanesha dkk, loc. cit

Berkaitan dengan Perlindungan Data Pribadi Nasabah dalam kaitannya dengan Tanggung Jawab Bank, sebetulnya telah ditemukan beberapa studi maupun kajian yang membahas mengenai hal tersebut. Namun, pada studi terdahulu memiliki fokus yang berbeda, misalnya seperti yang ditulis (1) Vanesha Marcelliana yang berfokus pada perlindungan konsumen akibat kasus kebocoran data pada PT. Bank Syariah Indonesia; kemudian (2) dalam studi yang ditulis oleh Vicky Katiandagho mengenai penguatan undang-undang data pribadi dalam perbankan; serta (3) studi yang ditulis oleh Subaidah Ratna Juita yang berfokus pada perlindungan nasabah dalam kejahatan *skimming*. Oleh karena itu, dapat di garis bawahi bahwa yang akan dibahas dalam penulisan kali ini memiliki fokus kajian yang berbeda dan penulis menuangkannya ke dalam jurnal dengan judul “Analisis Terhadap Tanggung Jawab Bank dalam Perlindungan Data Nasabah: Studi Kasus Perbankan Konvensional dan Perbankan Digital”.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang tersebut, rumusan masalah yang dapat dirumuskan dalam penelitian ini adalah bagaimana bentuk tanggung jawab bank dalam melindungi data nasabah, baik pada perbankan konvensional maupun perbankan digital, serta bagaimana perbandingan antara keduanya?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk memahami dan menganalisis tanggung jawab bank dalam melindungi data nasabah, baik pada perbankan konvensional maupun perbankan digital, serta membandingkan mekanisme perlindungan yang diterapkan pada keduanya. Selain itu, penelitian ini juga bertujuan menelaah efektivitas peraturan perundang-undangan yang berlaku di Indonesia, khususnya Undang-Undang Perlindungan Data Pribadi, dalam memberikan perlindungan data nasabah pada sektor perbankan.

II. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu metode yang menelaah hukum sebagai kaidah, norma, atau nilai yang berlaku di masyarakat dan menjadi pedoman perilaku bagi setiap orang. Dengan demikian, penelitian hukum normatif memusatkan perhatian pada analisis terhadap ketentuan hukum yang bersifat normatif⁷. Pendekatan normatif ini berarti bahwa penelitian berfokus pada penelaahan dokumen dan regulasi hukum yang berkaitan dengan tanggung jawab bank dalam melindungi data pribadi nasabah, baik pada bank konvensional maupun bank digital di Indonesia. Data yang digunakan meliputi data primer dan data sekunder, antara lain putusan pengadilan, peraturan perundang-undangan, literatur hukum, artikel jurnal, serta buku-buku yang relevan.

Selain itu, penelitian ini juga menerapkan pendekatan kualitatif untuk memperoleh pemahaman yang lebih mendalam mengenai praktik perlindungan data pribadi di lapangan. Penelitian ini turut menggunakan metode studi kasus melalui analisis jurnal dan artikel berita guna mengkaji kasus-kasus kebocoran data serta praktik perlindungan data yang dilakukan oleh bank. Dengan memadukan berbagai publikasi akademik dan laporan media, penelitian ini diharapkan dapat memberikan gambaran yang komprehensif dan sesuai kondisi nyata mengenai upaya perlindungan data pribadi yang diterapkan oleh bank di Indonesia.

⁷ Ishaq, I., Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, serta Disertasi, (Bandung, Alfabeta, 2017), 66.

III. Hasil dan Pembahasan

3.1 Analisis Tanggung Jawab Bank terhadap Perlindungan Data Nasabah

Tanggung jawab bank di Indonesia dalam melindungi data nasabah pada dasarnya telah diatur melalui berbagai peraturan perundang-undangan serta regulasi yang ditetapkan oleh otoritas yang berwenang. Bank-bank di Indonesia ini diwajibkan untuk selalu memastikan bahwa data pribadi setiap nasabah mereka dilindungi dari akses tanpa izin, penyalahgunaan, dan pengungkapan yang tidak sesuai. Beberapa regulasi utama yang mengatur perlindungan data nasabah di Indonesia meliputi Undang-Undang Nomor 21 Tahun 2011 tentang Sistem Informasi dan Data, Peraturan Otoritas Jasa Keuangan (POJK) Nomor 1/POJK.07/2013 yang mengatur tentang Pengelolaan Data Nasabah, serta standar keamanan informasi internasional seperti ISO/IEC 27001.

Ketentuan-ketentuan dalam peraturan tersebut pada dasarnya telah sangat lengkap dan memadai untuk menjamin keamanan data nasabah dari berbagai risiko apabila dilaksanakan dengan baik. Misalnya, Undang-Undang Nomor 21 Tahun 2011 telah mengatur prosedur pengumpulan dan pemanfaatan data pribadi nasabah, mengharuskan lembaga keuangan untuk menjaga data agar tidak diakses oleh pihak yang tidak berwenang, serta memberikan hak kepada nasabah untuk melihat dan memperbaiki data milik mereka⁸.

Selain itu, ada juga POJK Nomor 1/POJK.07/2013 menegaskan kewajiban bank untuk menjaga kerahasiaan data nasabah, memberikan transparansi mengenai penggunaan data, mengelola risiko terkait pengelolaan data, dan melakukan audit internal secara berkala. Kemudian ada juga ISO/IEC 27001 yang menyediakan kerangka kerja untuk mendirikan dan meningkatkan sistem manajemen keamanan informasi, melakukan penilaian risiko, menerapkan kontrol keamanan, dan memastikan kepatuhan terhadap hukum dan regulasi yang berlaku.

Dengan mematuhi regulasi yang berlaku, bank-bank di Indonesia, baik konvensional maupun digital, diharapkan dapat menjalankan kewajibannya yaitu bertanggung jawab dan mampu mengimplementasikan langkah-langkah keamanan yang efektif, termasuk penggunaan teknologi enkripsi, sistem deteksi intrusi, dan audit keamanan secara berkala. Seluruh upaya tersebut wajib dilakukan karena menjadi bagian dari tanggung jawab bank dalam menjaga dan melindungi data pribadi nasabah. Selain itu, mereka juga harus memastikan bahwa karyawan mereka dilatih dalam praktik terbaik perlindungan data supaya mereka juga mengetahui bahwa ada kebijakan internal yang ketat untuk mengelola akses data pribadi nasabah.

Namun, menurut hasil penelitian yang telah dilakukan, dalam hal perlindungan data nasabah ini dapat diketahui bahwa tanggung jawab bank masih memiliki beberapa kelemahan, baik dalam konteks perbankan konvensional maupun perbankan digital. Bank konvensional di Indonesia masih kurang memenuhi standar perlindungan data nasabah, terutama dalam pengumpulan dan penggunaan data pribadi.

Kelemahan-kelemahan tersebut terbukti masih sangat signifikan karena masih terjadi banyak kasus mengenai gagalnya bank dalam melindungi data pribadi milik nasabah. Dalam lima tahun terakhir, terdapat dua contoh kasus yang dapat dijadikan ilustrasi. Kasus pertama yaitu di tahun 2021 yang lalu, terdapat kebocoran data nasabah milik bank Jenius yang bernama Theresia Avila. Bank Jenius merupakan bank digital baru yang dibuat oleh PT Bank Tabungan Nasional Tbk (BTPN) dan resmi diperkenalkan pada publik tahun 2016 lalu. Dalam kasus ini, data pribadi nasabah, termasuk nomor telepon, alamat email, dan informasi rekening, dilaporkan telah sepenuhnya bocor. Kronologi

⁸ International Organization for Standardization. (2013). ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements. Geneva: International Organization for Standardization

terjadinya kasus tersebut diawali ketika Theresia Avila menerima panggilan telepon yang mengatasnamakan Jenius. Nomor telepon tersebut mengklaim bahwa terdapat pergantian kartu debit dan meminta Theresia untuk mengisi link yang diberikan. Theresia tidak merasa curiga karena ucapan yang disampaikan melalui nomor telepon tersebut memiliki kesamaan dengan gaya khas *customer service* Jenius. Kasus ini telah menimbulkan kekhawatiran bagi nasabah-nasabah lainnya tentang tingkat keamanan yang diterapkan oleh bank digital dan mendorong diskusi tentang perlunya peningkatan langkah-langkah perlindungan data di sektor perbankan digital.

Dalam mengatasi kasus tersebut, Jenius telah melakukan beberapa upaya penanganan, seperti menghubungi Theresia Avila untuk dapat melakukan investigasi lebih lanjut mengenai mengapa dapat terjadi kebocoran data pribadi tersebut. Selain itu, dari pihak OJK juga telah mengingatkan nasabah untuk menjaga kerahasiaan data, seperti tidak memberikan password kepada siapa pun, termasuk pegawai bank. Jenius juga melakukan investigasi menyeluruh terhadap kebocoran data dan memberikan perlindungan hukum kepada nasabah yang terkena dampak. Dalam kata lain, Jenius masih bertanggung jawab penuh atas hal yang terjadi terhadap nasabahnya.

Kemudian contoh kasus lainnya yang kedua adalah kasus kebocoran data yang menimpa Grace, nasabah bank BNI di tahun 2021 lalu. Informasi pribadi Grace mengenai transaksi keuangan beserta nomor rekeningnya tersebar di media sosial tanpa izinnnya sama sekali. Grace juga telah berusaha mengirimkan somasi kepada BNI Manado namun belum menerima respon sama sekali. Kejadian ini menimbulkan kekhawatiran Grace terhadap keamanan data nasabah di BNI Manado dan ia sangat berharap OJK dapat mengambil langkah untuk menanggapi masalah tersebut. Untuk kasus ini, Grace masih belum mendapatkan pertanggungjawaban yang adil dari pihak Bank maupun dari jalur hukum. Ini merupakan hal yang patut diprihatinkan karena membuktikan bahwa perlindungan data di bank BNI ini masih lemah.

Dari kasus kebocoran data yang telah dituliskan di atas, yang dialami oleh nasabah-nasabah seperti Theresia Avila dan Grace, dapat ditarik kesimpulan bahwa perlindungan data nasabah di sektor perbankan, baik konvensional maupun digital, masih memiliki kelemahan yang signifikan. Keduanya mengalami penyebaran informasi pribadi mereka tanpa izin di media sosial, menyoroti kebutuhan akan sistem keamanan yang lebih kuat dan edukasi yang lebih baik terhadap nasabah terkait taktik phishing dan keamanan data. Respons yang cepat dan efektif dari bank serta regulasi seperti OJK menjadi kunci dalam menangani dan mencegah kasus serupa di masa depan⁹. Peningkatan transparansi, akuntabilitas, dan perlindungan data yang lebih baik merupakan langkah krusial yang harus diambil oleh industri perbankan untuk memperbaiki standar keamanan dan mempertahankan kepercayaan nasabah¹⁰.

Jika ditelaah lebih mendalam, baik bank konvensional maupun digital masing-masing memiliki kelebihan dan kelemahan dalam hal keamanan. Dengan demikian, tidak ada yang bisa dikatakan lebih unggul secara mutlak, semua tergantung dari aspek apa yang nasabah perlukan, terutama dalam hal perlindungan data nasabah. Bank konvensional sering kali memiliki infrastruktur keamanan yang matang dan sistem yang telah teruji dari waktu ke waktu. Mereka juga biasanya memiliki tim keamanan yang dilatih khusus untuk menghadapi ancaman keamanan yang kompleks. Namun, bank

⁹ Sinaga, Guna Gerhat dkk. (2023). Analisis Peran Otoritas Jasa Keuangan terhadap Perbankan sebagai Upaya Perlindungan Data Pribadi Nasabah Bank (Studi Kasus Kebocoran Data Nasabah bank Syariah Indonesia). Jurnal Pendidikan Tambusai, 7(3), hlm. 28379

¹⁰ Yosefine. (2022). Perlindungan Hukum terhadap Nasabah BTPN Jenius Akibat Dugaan Kebocoran Data Pribadi Dihubungkan dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Fakultas Hukum Universitas Angeng Tirtayasa

konvensional mungkin lebih rentan terhadap risiko kesalahan manusia dan akses tidak sah karena skala operasi yang besar dan banyaknya sistem yang terpisah.

Di sisi lain, bank digital menawarkan teknologi keamanan yang lebih modern dan inovatif, seperti sistem deteksi ancaman canggih dan enkripsi data yang kuat. Mereka juga sering kali memiliki pendekatan yang lebih proaktif terhadap pengelolaan keamanan data nasabah. Namun, bank digital dapat lebih rentan terhadap serangan *cyber* seperti *phishing* dan *malware* karena sifat operasional mereka yang berbasis *online*.

3.2 Perbandingan Perlindungan Data Pribadi Nasabah antara Bank Konvensional dan Bank Digital

Baik bank konvensional maupun bank digital pada dasarnya memiliki kelebihan dan kelemahan masing-masing, meskipun keduanya terus mengalami perkembangan seiring dengan kemajuan teknologi saat ini. Di mata orang awam mungkin Bank Digital nampak lebih efektif, efisien, serta lebih meyakinkan dibandingkan Bank Konvensional dikarenakan berbagai pembaharuan yang telah dilakukan. Bank digital kerap dipandang lebih unggul dibandingkan bank konvensional karena menawarkan fitur keamanan yang lebih canggih serta didukung oleh teknologi yang lebih modern dalam menjaga data nasabah. Misalnya, Bank Digital memiliki sistem enkripsi data yang lebih efektif dan teknologi biometrik untuk verifikasi identitas sehingga tidak sembarang orang dapat mengakses data terutama data yang bersifat pribadi. Selain itu, bank digital juga memiliki sistem deteksi anomali yang lebih sensitif untuk mendeteksi transaksi mencurigakan. Oleh karena itu, bank digital dianggap lebih aman dalam melindungi data pribadi nasabah dibandingkan bank konvensional itu sendiri. Namun, sejatinya keberadaan Bank Digital justru memiliki risiko tinggi apabila tidak dilakukan *maintenance* maupun perkembangan sistem secara berkala. Pasalnya, seiring dengan berkembangnya teknologi, timbul oknum-oknum tidak bertanggung jawab yang senantiasa mencari celah untuk mendapatkan keuntungannya sendiri di tengah kemudahan teknologi yang telah ada. Risiko yang dapat timbul dalam dunia digitalisasi tidak akan jauh daripada *cybercrime* itu sendiri, di mana hal ini perlu untuk diwaspadai terutama bagi pemilik usaha bank digital. Dibutuhkan sistem keamanan yang kuat untuk meminimalkan risiko kebocoran data nasabah sehingga dapat meningkatkan rasa terlindungi dan nyaman bagi nasabah dalam menggunakan layanan bank.

Masing-masing memiliki kelemahannya tersendiri, seperti misalkan untuk bank konvensional di Indonesia masih menghadapi beberapa tantangan dalam melindungi data pribadi nasabah, seperti yang pertama yaitu dalam hal proses pengumpulan data pribadi nasabah sering kali tidak dilakukan dengan sistem yang terintegrasi dan aman. Ini dapat mengakibatkan potensi kebocoran data saat data tersebar di berbagai sistem internal yang tidak selalu terlindungi dengan baik. Kedua, tingkat kesadaran dan pelatihan terhadap karyawan bank tentang praktik keamanan data sering kali masih rendah, meningkatkan risiko kesalahan manusia atau akses tidak sah terhadap data nasabah. Ketiga, Penerapan teknologi keamanan tingkat lanjut, seperti enkripsi data maupun sistem deteksi ancaman, belum dilakukan secara merata oleh seluruh lembaga keuangan, sehingga masih terdapat celah bagi munculnya serangan yang lebih kompleks dan sulit terdeteksi.¹¹

Selanjutnya, kelemahan-kelemahan lainnya yang dimiliki oleh bank digital antara lain, seperti pertama, bank digital sering kali menjadi sasaran utama bagi para penjahat

¹¹ 11 Tarigan, Herdian Ayu dkk. (2019). Perlindungan Hukum terhadap Nasabah Atas Penyelenggaraan Terhadap Layanan Perbankan Digital. Jurnal Pembangunan Hukum Indonesia, 1(3), hlm. 305

cyber karena tingkat interaksi *online* yang tinggi. Hal ini membuat bank digital rentan terhadap serangan *phishing* dan *malware* yang dapat mengakibatkan pencurian data pribadi. Kedua, karena sifat operasional mereka yang berbasis online, bank digital harus menjaga agar infrastruktur mereka tetap aman dari serangan DDoS (*Distributed Denial of Service*) yang dapat menghambat operasional layanan dan memungkinkan akses tidak sah¹². Ketiga, dengan cepatnya inovasi teknologi dalam bank digital, sering kali terjadi keterlambatan dalam implementasi keamanan yang sesuai dengan perkembangan terbaru, meninggalkan celah keamanan yang perlu segera ditangani.

IV. Kesimpulan

Berdasarkan hasil penelitian, baik bank konvensional maupun bank digital memiliki kelebihan dan kekurangan dalam melindungi data pribadi nasabah. Bank digital menawarkan teknologi canggih dan efisiensi tinggi, namun rentan terhadap serangan siber jika tidak dikelola dengan baik. Sebaliknya, bank konvensional memiliki infrastruktur keamanan yang mapan dan tim terlatih, tetapi masih menghadapi tantangan dalam hal integrasi data dan risiko kesalahan manusia.

Kasus-kasus kebocoran data di beberapa bank menunjukkan bahwa perlindungan data di sektor perbankan masih memiliki kelemahan signifikan. Insiden-insiden ini menyoroti perlunya peningkatan keamanan data secara menyeluruh, baik dari segi teknologi maupun manajemen sumber daya manusia. Bank perlu memperkuat sistem keamanan siber mereka dan memastikan bahwa staf mereka memiliki pemahaman yang baik tentang praktik terbaik dalam perlindungan data.

Selain itu, perkembangan teknologi yang pesat memaksa bank untuk terus beradaptasi dan memperbarui sistem keamanan mereka. Bank digital, yang lebih cepat mengadopsi teknologi baru, harus memastikan bahwa inovasi tersebut tidak mengorbankan keamanan data nasabah. Di sisi lain, bank konvensional perlu lebih agresif dalam mengadopsi teknologi baru sambil tetap mempertahankan standar keamanan tinggi yang sudah ada.

Dari perbandingan antara bank konvensional dan digital, dapat disimpulkan bahwa tidak ada satu jenis bank yang secara mutlak lebih baik dalam hal keamanan data. Masing-masing jenis bank memiliki keunggulan dan tantangan tersendiri. Oleh karena itu, keputusan untuk memilih bank sebaiknya didasarkan pada kebutuhan dan preferensi pribadi nasabah, serta tingkat kenyamanan dan kepercayaan terhadap sistem keamanan yang ditawarkan oleh masing-masing bank.

Ke depan, bank perlu tidak hanya menitikberatkan pada aspek teknologi, tetapi juga pada edukasi dan peningkatan kesadaran keamanan di kalangan nasabah. Edukasi yang tepat akan membantu nasabah lebih berhati-hati terhadap ancaman seperti *phishing* dan penipuan *online*. Dengan demikian, kerja sama antara bank dan nasabah dalam menjaga keamanan data dapat berjalan lebih efektif.

Untuk meningkatkan perlindungan data nasabah, bank baik konvensional maupun digital disarankan untuk terus berinovasi dalam teknologi keamanan dan memperkuat sistem mereka terhadap potensi serangan siber. Selain itu, Bank wajib memastikan bahwa seluruh karyawannya menerima pelatihan yang cukup mengenai praktik-praktik terbaik dalam perlindungan data. Bank juga perlu meningkatkan transparansi dan akuntabilitas dalam menangani insiden keamanan, serta meningkatkan edukasi nasabah tentang pentingnya menjaga kerahasiaan informasi pribadi mereka. Langkah-langkah ini penting untuk

¹² Alhafiz, Muhammad Julda dkk. (2023). Dampak Denial of Service pada Perusahaan Perbankan di Indonesia. Jurnal Ilmu Multidisiplin, 2(1), hlm. 116

mempertahankan kepercayaan nasabah dan meningkatkan standar keamanan di industri perbankan.

Daftar Pustaka

- Alhafiz, Muhammad Julda dkk. (2023). Dampak Denial of Service pada Perusahaan Perbankan di Indonesia. *Jurnal Ilmu Multidisiplin*, 2(1), hlm. 116
- International Organization for Standardization. (2013). ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements. Geneva: International Organization for Standardization.
- Ishaq, I., Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, serta Disertasi, (Bandung, Alfabeta, 2017), 66.
- Kholis, Nur. (2018). Perbankan dalam Era Baru Digital, *Economicus: Jurnal Ekonomi dan Manajemen*, Universitas Sebelas Maret, 12(1)
- Marcelliana, Vanesha dkk. (2023). Penerapan Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia dalam Kasus Kebocoran Data Nasabah. *Jurnal Publikasi Ilmu Hukum*, 1(2), hlm. 182
- Putera, Andika Persada. (2020). Prinsip Kepercayaan Sebagai Fondasi Utama Kegiatan Perbankan. *Jurnal Hukum Bisnis Bonum Commune*, Lembaga Penelitian dan Pengabdian Masyarakat Universitas 17 Agustus 1945 Surabaya, 3 (1)
- Sinaga, Guna Gerhat dkk. (2023). Analisis Peran Otoritas Jasa Keuangan terhadap Perbankan sebagai Upaya Perlindungan Data Pribadi Nasabah Bank (Studi Kasus Kebocoran Data Nasabah bank Syariah Indonesia). *Jurnal Pendidikan Tambusai*, 7(3), hlm. 28379
- Tarigan, Herdian Ayu dkk. (2019). Perlindungan Hukum terhadap Nasabah Atas Penyelenggaraan Terhadap Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indonesia*, 1(3), hlm. 305
- Usanti, Trisandini dan Abd. Shomad. (2016). *Hukum Perbankan*. Prenamedia Group: Jakarta, hlm. 1
- Yosefine. (2022). Perlindungan Hukum terhadap Nasabah BTPN Jenius Akibat Dugaan Kebocoran Data Pribadi Dihubungkan dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Fakultas Hukum Universitas Ageng Tirtayasa.

Peraturan Perundang-Undangan

- Otoritas Jasa Keuangan. (2013). Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Pengelolaan Data Nasabah. Jakarta: Otoritas Jasa Keuangan.
- Pemerintah Republik Indonesia. (2011). Undang-Undang Republik Indonesia Nomor 21 Tahun 2011 tentang Sistem Informasi dan Data. Jakarta: Pemerintah Republik Indonesia.