JALAKOTEK: Journal of Accounting Law Communication and Technology
E-ISSN: 3032-2758 P-ISSN: 3032-3495
Vol. 2 No. 1 Januari 2025

Perlindungan Kepada Nasabah Bank Terhadap Kebocoran Data (Studi Kasus Kebocoran Data pada Bank Indonesia)

Angelina Jacqueline Sugiarto[1] Gunardi Lie[2] Moody Rizky Syailendra Putra[3]
Jurusan Hukum, Fakultas Hukum, Universitas Tarumanagara, Kota Jakarta Barat, Provinsi DKI Jakarta, Indonesia[1,2,3]
Email: angelina.205230021@untar.ac.id[1] gunardi.lie@untar.ac.id[2] moodys@fh.untar.ac.id[3]

Abstrak

Kemajuan teknologi digital banking memberikan banyak dampak ada dampak positif, namun kemajuan teknologi digital banking juga memberikan dampak negatif, terutama dalam hal kebocoran data dalam perbankan. Kasus atas kebocoran data nasabah di Bank Syariah Indonesia menjadi salah satu contoh nyata dari masalah kebocoran data dalam perbankan di Indonesia. Studi ini bertujuan menganalisis perlindungan hukum kemudian upaya hukum dalam menghadapi kebocoran data nasabah pada sistem perbankan. Metode penelitian yang digunakan adalah metode normatif dan kualitatif, dengan pendekatan analisis hukum mengenai perundang-undangan yang berlaku di Indonesia dan relevan dengan kasus. Hasil penelitian menunjukkan bahwa meskipun terdapat perlindungan hukum di Indonesia yang sangat ketat kasus kebocoran data dalam perbankan masih sering terjadi. Untuk memenuhi tanggung jawab untuk melindungi data dan mencegah kebocoran data yang serupa, bank perlu menerapkan atau melaksanakan upaya-upaya melindungi kerahasian data nasabah termasuk penerapan enkripsi data, penggunaan teknologi blockchain dan audit keamanan secara berkala. Selain itu, bank harus memberikan pelatihan keamanan data kepada karyawan, menandatangani perjanjian kerahasiaan dengan karyawan, vendor dan mitra, serta menyediakan mekanisme laporan kebocoran data bagi nasabah. Kesimpulannya, perlindungan hukum yang ada harus diimbangi dengan upaya yang lebih dari pihak perbankan dalam menjaga kerahasian data nasabah. Dengan demikian, kepercayaan nasabah terhadap institusi perbankan dapat tetap terjaga, kemudian risiko kebocoran data dapat diminimalisir dan dapat menciptakan lingkungan perbankan terpercaya dan aman.
Kata Kunci: Kebocoran Data, Digital Banking, Perlindungan Hukum, Bank Syariah Indonesia

Abstract

The advancement of digital banking technology has many impacts, including positive effects, but it also brings negative consequences, especially regarding data breaches in banking. The case of data breaches involving customers at Bank Syariah Indonesia is a concrete example of the data breach problem in banking in Indonesia. This study aims to analyze legal protections and legal measures in addressing customer data breaches within the banking system. The research methodology employed is normative and qualitative, using a legal analysis approach regarding the legislation in force in Indonesia that is relevant to the case. The findings indicate that despite strict legal protections in Indonesia, data breaches in banking still frequently occur. To fulfill their responsibility to protect data and prevent similar breaches, banks need to implement measures to safeguard customer data confidentiality, including data encryption, the use of blockchain technology, and regular security audits. Additionally, banks must provide data security training to employees, sign confidentiality agreements with employees, vendors, and partners, and establish mechanisms for customers to report data breaches. In conclusion, existing legal protections must be complemented by greater efforts from banking institutions to maintain the confidentiality of customer data. Thus, customer trust in banking institutions can be upheld, the risk of data breaches can be minimized, and a trustworthy and secure banking environment can be created.
Keywords: *Data Breaches, Digital Banking, Legal Protection, Bank Syariah Indonesia*

PENDAHULUAN

Perlindungan kepada nasabah bank terhadap kebocoran data menjadi semakin krusial seiring dengan pesatnya perkembangan teknologi digital. Dalam era digital ini, bank menghadapi banyak tantangan-tantangan yang besar untuk menjaga data pribadi nasabah. Salah satunya *digital banking, digital banking* menawarkan kemudahan dan aksesibilitas, tetapi tidak menutup kemungkinan bisa mengalami kebocoran data. Adanya kebocoran data dapat berakibat fatal, tidak hanya bagi individu, tetapi juga bagi reputasi lembaga perbankan itu sendiri. Oleh karena itu, bank perlu menerapkan berbagai langkah proaktif untuk melindungi informasi sensitif yang dimiliki. Regulasi dan kebijakan yang ketat harus diterapkan untuk memberikan kerangka hukum yang jelas dalam pengelolaan data nasabah. Semua ini bertujuan untuk menciptakan kepercayaan di kalangan nasabah dan menjaga integritas sistem perbankan. Isu kebocoran data telah menjadi perhatian utama di seluruh dunia, termasuk Indonesia. Dalam beberapa tahun terakhir, sejumlah kasus kebocoran data di sektor perbankan telah mengungkapkan betapa rentannya informasi pribadi nasabah. Kebocoran ini sering kali disebabkan oleh serangan siber, kurangnya keamanan sistem, atau bahkan kelalaian dari pihak internal bank. Ketika data sensitif seperti nomor rekening, *password*, dan informasi pribadi lainnya bocor, dampaknya bisa sangat merugikan bagi nasabah. Kerugian finansial, pencurian identitas, dan penurunan kepercayaan terhadap lembaga keuangan adalah beberapa konsekuensi yang sering terjadi. Selain itu, lembaga perbankan yang mengalami kebocoran data juga berisiko menghadapi sanksi dari regulator dan kerugian reputasi yang sulit dipulihkan. Ini menggarisbawahi pentingnya perlindungan data yang efektif dan berkelanjutan.

Salah satu contoh nyata dari isu kebocoran data di sektor perbankan adalah kasus yang melibatkan Bank Syariah Indonesia (BSI). Pada tanggal 8 Mei 2023, seluruh layanan BSI terhenti akibat serangan siber, yang membuat nasabah tidak dapat melakukan transaksi apapun. Penutupan layanan ini berdampak luas, termasuk pada jaringan ATM, *mobile banking,* dan kantor cabang. Setelah penyelidikan, terungkap bahwa insiden tersebut berkaitan dengan serangan dari kelompok *hacker* LockBit 3.0. Mereka berhasil mengakses dan mengenkripsi data nasabah, sehingga menyebabkan kebocoran informasi sensitif. Banyak nasabah mengeluh kehilangan dana dan merasa terancam akibat kebocoran data ini. Kasus ini menyadarkan betapa pentingnya tindakan pencegahan dan respons cepat dalam menghadapi ancaman siber. Menurut Alfons, peretasan ini kemungkinan dilakukan lebih awal, yakni saat libur Idul Fitri. Alfons mengatakan insiden itu mungkin terjadi sebelum tanggal 8 Mei 2023, karena disaat itu data-data dari pelanggan BSI sudah berhasil disalin dan dienkripsi. Kebocoran data ini menimbulkan kerugian terhadap nasabah selain kebocoran data nasabah juga kehilangan dana nya. Saya memilih kasus ini untuk menelusuri lebih dalam mengenai perlindungan hukum bagi nasabah ketika terjadi kebocoran data, serta untuk mengeksplorasi upaya bank dalam menjaga kerahasiaan data nasabah. Besar harapan saya sebagai penulis agar makalah ini dapat bermanfaat bagi pembaca. Rumusan Masalah: Bagaimana perlindungan perbankan terhadap nasabah jika mengalami kebocoran data? Bagaimana tanggung jawab bank dalam melindungi atau menjaga kerahasiaan data nasabah dalam penggunaan *digital banking*?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian normatif. Penelitian Normatif yaitu penelitian yang memproses tentang aturan - aturan hukum yang berlaku yang sudah ada guna menjawab kasus terkait hukum yang dibahas dalam jurnal penelitian ini.

Desain Penelitian

Penelitian ini menggunakan metode kualitatif. Penelitian kualitatif adalah metode penelitian yang bertujuan menjelaskan fenomena dengan mendalam. Dalam penelitian ini, penulis berupaya menggambarkan masalah dengan mengamati, menguraikan, dan mendeskripsikan masalah hukum tentang bagaimana perlindungan hukum perbankan terhadap nasabah jika mengalami kebocoran data dalam bertransaksi dan bagaimana upaya bank melindungi atau menjaga kerahasiaan data nasabah dalam penggunaan *digital banking*

Sumber Data

1. Data Primer. Penulis mencari dan mengumpulkan data primer seperti perundang-undangan, dan putusan hakim. Adapun yang penulis gunakan adalah:
   a. Undang-Undang No.10 Tahun 1998
   b. Undang-Undang No. 8 Tahun 2010
   c. HIR
2. Data Sekunder. Data sekunder berupa mengacu pada semua publikasi seperti teori, dokumen, jurnal hukum, serta komentar terhadap keputusan pengadilan dan karya ilmiah yang terkait dengan jurnal ini.
3. Data Tersier. Data tersier merupakan bahan yang membantu menyempurnakan uraian data primer dan data sekunder, contohnya materi media internet yang terkait dengan jurnal ini.

Metode Pengumpulan Data

Pengumpulan data-data dicerna dengan metode melakukan kegiatan seperti penelitian kepustakaan,khususnya membaca, dan menelaah apa yang ada di peraturan perundang-undangan yang berhubungan dengan pokok permasalahan.

Pengolahan dan Analisis

1. Pengolahan
   a. Mengedit, dilakukan dengan penulis mengkaji bahan hukum yang diperoleh melengkapi bahan/ data hukum yang tidak lengkap, dan mengedit bahan tersebut menjadi kalimat yang lebih baik.
   b. Sistematis, dilakukan dengan menyeleksi bahan/data hukum, mengklasifikasikannya.
   c. Mendeskripsikan, dilakukan dengan penulis merangkumkan dan menjelaskan temuan berdasarkan dokumen yang ada.
2. Analisis. Data-data ini memakai analisis kualitatif penelitian yang menjelaskan fenomena dengan mendalam.

HASIL PENELITIAN DAN PEMBAHASAN

Bagaimana perlindungan hukum perbankan terhadap nasabah jika mengalami kebocoran data?

Di Indonesia memiliki beberapa peraturan-peraturan yang mengatur mengenai perlindungan hukum perbankan terhadap nasabah jika mengalami kebocoran data. Perlindungan hukum perbankan terhadap nasabah jika mengalami kebocoran data diatur oleh Pasal 40 (1) UU No.10 Tahun 1998 yang berbunyi: "(1) Bank wajib merahasiakan keterangan mengenai nasabah penyimpanan dan simpanannya kecuali dalam hal sebagaimana dimaksud Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44A". Pasal 40 ayat (1) UU No. 10 Tahun 1998 tentang Perbankan mewajibkan bank untuk menjaga kerahasiaan informasi

mengenai nasabah dan simpanannya, Namun, ada beberapa pengecualian yang memungkinkan bank untuk membuka informasi nasabah, seperti untuk kepentingan perpajakan, penegakan hukum terkait tindak pidana, sengketa antara bank dan nasabah, serta pengelolaan piutang negara. Pengecualian ini berlaku misalnya dalam kasus pencucian uang tindak pidana, yang memiliki ketentuan rahasia bank bisa diterobos demi kepentingan penyidikan oleh otoritas yang berwenang seperti yang diatur dalam UU TPPU (Undang-Undang No. 8 Tahun 2010). Jika terjadi kebocoran data di luar konteks pengecualian tersebut, bank dapat dianggap melanggar kewajiban mereka terhadap prinsip kerahasiaan. Dalam situasi ini, nasabah memiliki hak untuk menuntut bank atas kerugian yang diakibatkan, baik melalui jalur perdata maupun pidana. Perlindungan hukum bagi nasabah juga diatur dalam berbagai mekanisme lain, seperti penyediaan informasi risiko dan perlindungan simpanan melalui Lembaga Penjamin Simpanan (LPS), yang sudah diatur dalam Pasal 37B UU No. 10 Tahun 1998.Perlindungan hukum perbankan terhadap nasabah jika mengalami kebocoran data juga ada di Peraturan Bank Indonesia Nomor 7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi. Peraturan tersebut mengatur tentang transparansi informasi produk bank dan penggunaan data pribadi.

Peraturan ini menekankan pentingnya menjaga kerahasian data pribadi nasabah dan mengatur sanksi bagi bank yang melanggar peraturan tersebut. Selain itu peraturan Otoritas Jasa Keuangan (OJK) juga mengatur tentang perlindungan konsumen,termasuk data pribadi nasabah yang harus dirahasiakan dan tidak boleh diberikan kepada pihak ketiga tanpa persetujuan nasabah. Dalam beberapa kasus, banyak peraturan-peraturan yang belum sepenuhnya dilaksanakan, sehingga masih banyak nasabah yang merasa khawatir akan bocornya data pribadi miliknya. Seperti kasus yang belakangan ini terjadi yaitu Bank Syariah Indonesia (BSI). Layanan *digital banking* Bank Syariah Indonesia (BSI) ini mengalami gangguan pada hari Senin 8 Mei 2023 di seluruh Indonesia sehingga nasabah tidak bisa melakukan transaksi apapun. Gangguan layanan Bank Syariah Indonesia (BSI) ini berimbas pada jaringan *ATM*, *mobile banking,* dan kantor perusahaan yang tidak bisa diakses. Gangguan layanan ini berlangsung selama 4 hari.Bank Syariah Indonesia (BSI) menyelidiki apa yang menyebabkan gangguan tersebut terjadi lalu ditemukkan adanya indikasi atas serangan viber. Pada tanggal 11 Mei 2023 Bank Syariah Indonesia (BSI) kembali normal. Banyaknya nasabah Bank Syariah Indonesia (BSI) yang mengeluh kehilangan dana. Diselidiki lebih dalam terdapat kebocoran sejumlah data dan *password* nasabah Bank Syariah Indonesia (BSI). Prediksi kronologi kelompok *hacker LockBit 3.0* melakukan peretasan terhadap Bank Syariah Indonesia (BSI). *LockBit* merupakan salah satu geng *ransomware* yang aktif dan berbahaya.

Sejumlah perusahaan di beberapa negara juga sempat menjadi korban penyerangan ini. Dikatakan bahwa insiden itu mungkin terjadi sebelum 8 Mei 2023, karena pada saat itu data pelanggan BSI sudah berhasil disalin dan dienkripsi. Artinya keamanan pada Bank Syariah Indonesia (BSI) kurang aman karena seperti yang dikatakan Alfons sebelum tanggal 8 sudah bocor bagaimana Bank Syariah Indonesia (BSI) tidak mengetahui hal tersebut. Dampak dari kebocoran data ini menimbulkan kerugian terhadap nasabah kehilangan dana selain nasabah juga kebocoran data. Kasus dari Bank Syariah Indonesia (BSI) ini hanya salah satu kasus dari banyaknya kasus kebocoran data di perbankan. Banyaknya kasus kebocoran data dalam perbankan ini harus ditindaklanjuti lebih dalam mengingat kebocoran data ini memiliki dampak yang sangat besar. Oleh karena itu, penting bagi bank untuk menjaga kerahasian data pribadi nasabah dalam bentuk apapun agar terhindar dari kebocoran data.

Bagaimana tanggung jawab bank dalam melindungi atau menjaga kerahasiaan data nasabah dalam penggunaan *digital banking?*

Akar dari permasalahan kebocoran data nasabah ini bisa berasal dari sumber eksternal maupun internal. Misalnya, kesalahan manusia yang secara tidak sengaja mengakses informasi rahasia secara *online.* Sumber kebocoran data lainnya seperti malware atau penyusup melalui email,unduhan internet, atau program yang terinfeksi. Seperti apa yang terjadi pada kasus Bank Syariah Indonesia (BSI). Agar tidak kembali terjadinya kasus kebocoran data yang sama seperti Bank Syariah Indonesia (BSI). Bank wajib memiliki tanggung jawab untuk melindungi kerahasian data nasabah dalam penggunaan *digital banking*. Tanggung jawab bank tersebut berupa mengamankan data, kepatuhan regulasi, pelatihan karyawan, transparansi, pengelolaan yang baik mengenai masalah bank, penyimpanan data, audit dan pemantauan. Dengan tanggung jawab bank tersebut lahirlah upaya-upaya untuk mengatasi kebocoran data dan menjaga kerahasian data nasabah. Upaya bank dalam melindungi atau menjaga kerahasian data nasabah meliputi beberapa strategi,seperti enkripsi data. Enkripsi data mengamankan data dengan cara mengubah data menjadi format yang tidak dapat dibaca, yaitu *ciphertext.* Enkripsi data sangat penting dalam industri perbankan karena memiliki tiga faktor keamanan utama: kerahasiaan,integritas, otentikasi.

Kerahasian memastikan bahwa hanya pihak yang berwenang yang memiliki akses terhadap informasi sensitif. Enkripsi melindungi informasi pribadi dan keuangan pelanggan,seperti nomor rekening,kata sandi,dan rincian transaksi dari akses yang tidak sah. Integritas memastikan bahwa data tidak rusak atau diubah selama transmisi atau penyimpanan. Enkripsi melindungi data dari perubahan yang tidak sah yang membuat data terenkripsi tidak dapat dibaca atau digunakkan, menjaga keakuratan informasi,mencegah penipuan, dan memperkuat kepercayaan antar bank dan nasabah. Otentikasi memastikan bahwa pihak yang mengirim dan menerima data adalh entitas yang sah. Enkripsi membantu memverifikasi identitas semua pihak yang terlibat dalam suatu transaksi, mencegah pencurian identitas, dan memastikan bahwa data hanya dibagikan pada entitas yang berwenang. Selain itu, enkripsi juga dapat membantu bank memenuhi persyaratan peraturan seperti GDPR dan PCI DSS, yang memerlukan perlindungan data pelanggan dan mengenakan sanksi tegas atas pelanggaran. Dengan menerapkan enkripsi yang kuat, bank menunjukkan komitmen mereka terhadap keamanan data dan melindungi diri dari risiko hukum dan keuangan. Secara keseluruhan, enkripsi data merupakan bagian penting dari keamanan perbankan. Melindungi informasi sensitif, menjaga integritas data, memastikan otentikasi, dan membantu bank mematuhi peraturan. Seiring kemajuan teknologi dan meningkatnya ancaman dunia maya, enkripsi terus menjadi alat pertahanan penting untuk melindungi data nasabah dan kepercayaan terhadap industri perbankan.

Kemudian penggunaan teknologi *blockchain.* Penggunaan *blockchain* ini guna untuk mencatat setiap transaksi atau pertukaran dalam blok yang aman tidak mudah diubah, berkat teknik kriptografi. Setelah verifikasi, setiap blok ditautkan secara kriptografis ke blok sebelumnya melalui hash. Hash ini menyimpan data berupa tanda tangan digital atau sidik jari yang mengidentifikasi blok dan isinya dengan kode unik tertentu. Sistem ini memberikan perlindungan data yang sangat baik karena setiap transaksi diverifikasi oleh penambang sebelum diproses oleh banyak komputer. Struktur database ini sudah terenkripsi.Artinya, hanya bisa menambahkan data, tidak bisa mengeditnya. Riwayat transaksi dienkripsi dan tidak dapat diubah, sehingga meminimalkan penipuan. Selain itu, *blockchain* menyediakan sistem audit yang lebih baik, memungkinkan siapa saja untuk melihat dan melacak data transaksi dan

jejak audit aset. Dengan berbagai manfaat tersebut, *blockchain* memiliki potensi besar untuk mentransformasi model dan proses bisnis di industri jasa keuangan. *Blockchain* juga dapat menyederhanakan operasi dengan mengotomatiskan identifikasi pelanggan dan mempercepat proses kliring dan penyelesaian transaksi.

Banyak upaya-upaya lain yang bisa bank lakukan untuk mencegah kebocoran data dan melindungi data nasabah selain enkripsi data dan penggunaan *blockchain* seperti melakukan audit keamanan secara berkala. Bank perlu melakukan audit secara berkala untuk menilai efektivitas kebijakan keamanan data dan untuk memastikan bahwa semua sistem dan proses berjalan sesuai dengan standar yang telah ditetapkan. Memberikan pelatihan keamanan data kepada karyawan. Karyawan bank perlu mendapatkan pelatihan yang cukup tentang kebijakan keamanan data dan perlindungan privasi, sehingga mereka dapat memahami dan mengimplementasikan langkah-langkah yang diperlukan untuk menjaga kerahasiaan data nasabah. Bank juga harus memberikan transparansi seperti memberikan informasi yang jelas kepada nasabah mengenai bagaimana data mereka digunakan, disimpan, dan dilindungi. Nasabah juga harus diberi tahu tentang hak-hak mereka terkait data pribadi. Bank diharuskan juga untuk mematuhi peraturan perundang-undangan yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, yang mengharuskan lembaga keuangan untuk menjaga kerahasiaan dan keamanan data nasabah.Bank harus memiliki rencana tanggap darurat untuk menghadapi kebocoran data atau insiden keamanan lainnya. Ini termasuk prosedur untuk memberitahukan nasabah yang terkena dampak dan langkah-langkah yang diambil untuk mencegah kejadian serupa di masa depan. Data nasabah harus disimpan dengan aman dan hanya untuk periode yang diperlukan. Setelah tidak lagi diperlukan, data tersebut harus dihapus dengan cara yang aman.

KESIMPULAN

Bank secara besar memiliki tanggung jawab untuk mencegah kebocoran data. Di Indonesia, perlindungan perbankan terhadap nasabah dalam kasus kebocoran data diatur oleh beberapa ketentuan hukum, termasuk Pasal 40 (1) UU No. 10 Tahun 1998, yang mewajibkan bank untuk menjaga kerahasiaan informasi nasabah dan simpanannya. Kasus BSI, yang melibatkan serangan *ransomware* oleh kelompok Lock Bit 3.0, mengungkapkan bahwa data nasabah dapat bocor sebelum gangguan terjadi, mengindikasikan adanya kelemahan dalam sistem keamanan bank. Insiden kebocoran data seperti yang terjadi pada Bank Syariah Indonesia (BSI) pada Mei 2023 menunjukkan bahwa meskipun ada peraturan yang ketat tetap saja bisa terjadi kebocoran data. Untuk mencegah kebocoran data, bank perlu menerapkan berbagai strategi perlindungan data. Salah satu upaya penting adalah enkripsi data, yang memastikan kerahasiaan, integritas, dan otentikasi informasi. Enkripsi melindungi data dari akses yang tidak sah, memastikan data tidak rusak atau diubah, dan memverifikasi identitas pihak yang terlibat dalam transaksi. Selain itu, enkripsi membantu bank memenuhi regulasi seperti GDPR dan PCI DSS, yang menetapkan standar perlindungan data pelanggan.Teknologi *blockchain* juga menawarkan solusi tambahan dengan mencatat transaksi dalam blok yang terenkripsi dan tidak dapat diubah setelah diverifikasi. Ini memberikan perlindungan data yang kuat dan sistem audit yang transparan, yang dapat meningkatkan efisiensi dan keamanan dalam transaksi keuangan.Selain enkripsi data dan penggunaan *blockchain*, bank juga perlu melakukan audit keamanan secara berkala, memberikan pelatihan keamanan data kepada karyawan, menandatangani perjanjian kerahasiaan dengan pihak terkait, dan menyediakan mekanisme laporan kebocoran data untuk nasabah. Upaya-upaya ini penting untuk menjaga

kerahasiaan data nasabah dan menghindari kebocoran yang dapat berdampak negatif pada kepercayaan dan keamanan industri perbankan.

Saran

1. Meningkatkan kembali keamanan data pribadi nasabah
2. Menggunakan teknologi-teknologi baru untuk menjaga keamanan data nasabah
3. Melakukan audit keamanan secara berkala
4. Bank bertanggung jawab atas kebocoran data nasabah

Ucapan Terima Kasih

Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan bantuan dalam proses pembuatan makalah penelitian ini:

1. Prof. Dr. Gunardi Lie, S.H., M.H. dan Moody Rizky Syailendra P. S.H., M.H. sebagai dosen pembimbing yang telah memberikan bimbingan dan arahan berharga dalam penulisan makalah ini.
2. Keluarga besar penulis yang telah memberikan dukungan baik secara materi maupun moral, serta semangat untuk menyelesaikan makalah penelitian ini.
3. Semua teman-teman yang telah mendukung selama proses pembuatan makalah ini.

Akhir kata sebagai penulis, saya berharap makalah penelitian ini dapat memberikan manfaat bagi pembaca dan peneliti lainnya.

DAFTAR PUSTAKA

Anwar, M. (2020). "Perlindungan Hukum Terhadap Nasabah Bank Dalam Kasus Kebocoran Data Pribadi." *Jurnal Hukum & Pembangunan*, 50(1), 123-138.

Bisnis.com. (2023). Kronologi BSI diserang ransomware oleh hacker LockBit 3.0 diduga beraksi sejak libur Lebaran 2023. Diakses dari https://finansial.bisnis.com/read/20230514/90/1655733/kronologi-bsi-diserang-ransomware-oleh-hacker-lockbit-30-diduga-beraksi-sejak-libur-lebaran-2023

BRI. (n.d.). Perbankan digital: Pengertian, manfaat, hingga tantangannya. Diakses dari https://developers.bri.co.id/id/news/perbankan-digital-pengertian-manfaat-hingga-tantangannya

Budiarto, S. (2022). "Perlindungan Data Nasabah di Era Digital: Tinjauan Hukum." *Jurnal Ilmu Hukum*, 15(3), 221-235.

Chen, L. (2022). "The Impact of Data Breaches on Consumer Trust in Banking Institutions." *Journal of Financial Regulation and Compliance*, 30(1), 45-60.

Futureskills. (n.d.). Keamanan data nasabah perbankan. Diakses dari https://futureskills.id/blog/keamanan-data-nasabah-perbankan/

Hukum Online. (n.d.). Langkah hukum jika data keuangan nasabah bocor. Diakses dari https://www.hukumonline.com/klinik/a/langkah-hukum-jika-data-keuangan-nasabah-bocor-lt653e1e9d6d9c4/

Insightful Banking. (n.d.). Data privacy in digital banking. Diakses dari https://insightfulbanking.com/data-privacy-in-digital-banking-2/

Johnson, R., & Lee, H. (2020). "Cybersecurity in Banking: Protecting Consumer Data." *Journal of Banking Regulation*, 21(4), 300-317.

JPTAM. (n.d.). Perlindungan data pribadi dalam perbankan digital. Diakses dari https://jptam.org/index.php/jptam/article/download/11404/8910/21029

Jurnal Syntax Admiration. (n.d.). Analisis yuridis perlindungan hukum data. Diakses dari https://jurnalsyntaxadmiration.com/index.php/jurnal/article/download/964/1387/8495

Mahkamah Agung Republik Indonesia. (n.d.). Putusan perkara nomor: 11ead20410595760a072303832393038. Diakses dari https://putusan3.mahkamahagung.go.id/peraturan/detail/11ead20410595760a072303832393038.html

Meniga. (n.d.). Data privacy in digital banking. Diakses dari https://www.meniga.com/resources/data-privacy-in-digital-banking/

Miller, A., & Roberts, T. (2019). "Challenges in Data Privacy for Financial Institutions." *Financial Services Review*, 28(2), 119-133.

Neliti. (n.d.). Analisis yuridis perlindungan hukum data. Diakses dari https://media.neliti.com/media/publications/209693-analisis-yuridis-perlindungan-hukum-data.pdf

New Softwares. (n.d.). How do banks encrypt data?.Diakses dari https://www-newsoftwares-net.translate.goog/blog/how-do-banks-encrypt-data/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=rq

OJK. (n.d.). Kelebihan layanan perbankan digital dalam bertransaksi dan otorisasi. Diakses dari https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/40702

OJK. (n.d.). SE OJK 14: Kerahasiaan data dan informasi. Diakses dari https://www.ojk.go.id/id/regulasi/Documents/Pages/SEOJK-tentang-Kerahasiaan-dan-Keamanan-Data-dan-atau-Informasi-Pribadi-Konsumen/SE%20OJK%2014.%20Kerahasiaan%20Data%20dan%20Informasi.pdf

Prasetyo, A. (2021). "Kebocoran Data Nasabah dan Implikasinya Terhadap Kepercayaan Publik." *Jurnal Perbankan dan Hukum*, 7(2), 67-82.

ResearchGate. (2023). Personal data protection law in digital banking governance in Indonesia. Diakses dari https://www.researchgate.net/publication/369871741_Personal_Data_Protection_Law_in_Digital_Banking_Governance_in_Indonesia

Sari, R. (2019). "Tanggung Jawab Hukum Bank Dalam Melindungi Data Pribadi Nasabah." *Jurnal Hukum dan Teknologi*, 8(1), 45-58.

Undip. (n.d.). Perlindungan data dan informasi pribadi nasabah. Diakses dari https://ejournal3.undip.ac.id/index.php/dlr/article/view/12557

Universitas Airlangga. (n.d.). Privasi data dalam perbankan digital. Diakses dari https://all.fh.unair.ac.id/index.php?id=21592&p=show_detail

Universitas Indonesia. (n.d.). Data perlindungan di perbankan. Diakses dari https://lib.ui.ac.id/detail?id=20514034&lokasi=lokal

Universitas Pattimura. (n.d.). Perlindungan hukum data dalam perbankan digital. Diakses dari https://opac.fhukum.unpatti.ac.id/index.php?bid=8329&fid=7338&p=fstream-pdf

Wulandari, T. (2023). "Analisis Perlindungan Hukum Nasabah Terhadap Kebocoran Data." *Jurnal Hukum dan Kebijakan Publik*, 12(4), 333-348.