KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.1, No.6 Desember 2024
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 129-135
DOI: https://doi.org/10.61722/jmia.v1i6.2885

Tanggung Jawab Hukum Bank dalam Kasus Kebocoran Data Nasabah

Syafa Widya Annafa
Universitas Negeri Semarang
Hanintya Pasha Gabriel Hasa Simanjuntak
Universitas Negeri Semarang
Meira Ananda Ayudia
Universitas Negeri Semarang
Alamat: Kampus UNNES, Sekaran, Kec. Gn. Pati, Kota Semarang, Jawa Tengah
Korespondensi penulis: syafawidya@students.unnes.ac.id

Abstrak. *This research examines the legal responsibilities of banks in cases of customer data breaches in Indonesia. The study aims to analyze the scope of the banks' legal obligations, the mechanisms for protecting customer data, and to evaluate data breach cases in order to formulate recommendations for strengthening the system. Using a normative legal research method, this study investigates relevant regulations, banking practices, and case studies. The findings indicate that banks have multi-layered responsibilities based on various laws, while existing protection mechanisms often prove inadequate in preventing sophisticated cyber threats. This research also provides practical recommendations for enhancing data protection systems in the banking sector.*
Keywords: *banking law; cybersecurity; data protection; financial privacy; legal liability.*

Abstrak. Penelitian ini menganalisis tanggung jawab hukum bank terkait kebocoran data nasabah di Indonesia. Tujuan dari penelitian ini adalah untuk mengkaji ruang lingkup kewajiban hukum bank, mekanisme perlindungan data nasabah, serta mengevaluasi kasus kebocoran data guna merumuskan rekomendasi untuk memperkuat sistem. Dengan menggunakan metode penelitian hukum normatif, studi ini meneliti peraturan yang relevan, praktik perbankan, dan studi kasus. Hasil penelitian menunjukkan bahwa bank memiliki tanggung jawab yang berlapis berdasarkan berbagai undang-undang, sementara mekanisme perlindungan yang ada sering kali tidak cukup efektif dalam menghadapi ancaman siber yang kompleks. Penelitian ini juga memberikan rekomendasi praktis untuk memperkuat sistem perlindungan data di sektor perbankan
Kata Kunci: *hukum perbankan; keamanan siber; perlindungan data; privasi keuangan; tanggung jawab hukum.*

PENDAHULUAN

Era digitalisasi perbankan telah membawa perubahan besar dan transformasi signifikan dalam layanan keuangan, yang memungkinkan bank untuk menawarkan berbagai inovasi dan kemudahan bagi nasabah, seperti transaksi *online*, *mobile banking*, dan layanan perbankan berbasis aplikasi. Namun, perkembangan ini juga diiringi dengan munculnya tantangan baru, khususnya terkait dengan keamanan data pribadi nasabah. Maraknya kasus kebocoran data nasabah bank di Indonesia dalam beberapa tahun terakhir menunjukkan adanya kesenjangan yang signifikan antara pesatnya perkembangan teknologi dengan kesiapan sistem perlindungan data yang diterapkan oleh industri perbankan. Berdasarkan data yang dihimpun oleh Otoritas Jasa Keuangan (OJK), sepanjang periode 2020 hingga 2023 telah dilaporkan lebih dari 20 kasus kebocoran data nasabah di berbagai bank, yang menyebabkan kerugian finansial bagi nasabah maupun lembaga perbankan dengan estimasi total mencapai triliunan rupiah.

Analisis kesenjangan (*gap analysis*) terhadap regulasi yang berlaku menunjukkan bahwa meskipun telah ada aturan yang mewajibkan bank untuk melindungi data nasabah sesuai standar

Received September 30, 2024; Revised Oktober 30, 2024;Desember 01, 2024
* Syafa Widya Annafa, syafawidya@students.unnes.ac.id

keamanan tertentu, implementasi di lapangan sering kali menghadapi berbagai kendala, baik yang bersifat teknis maupun operasional. Tantangan tersebut mencakup kurangnya sumber daya yang memadai, infrastruktur teknologi yang belum optimal, serta rendahnya kesadaran akan pentingnya perlindungan data di tingkat operasional. Selain itu, dinamika ancaman siber yang terus berkembang, seperti *phishing*, *malware*, dan serangan *hacking*, semakin memperumit upaya perlindungan data nasabah.

Dalam konteks ini, penelitian ini bertujuan untuk menganalisis secara mendalam tanggung jawab hukum yang harus dipenuhi oleh bank dalam menghadapi kasus kebocoran data nasabah. Selain itu, penelitian ini juga berupaya merumuskan rekomendasi yang dapat membantu memperkuat sistem perlindungan data di sektor perbankan Indonesia, dengan mempertimbangkan aspek regulasi, teknologi, dan praktik operasional yang terbaik. Harapannya, hasil penelitian ini dapat memberikan kontribusi bagi peningkatan keamanan data nasabah dan mendorong terciptanya ekosistem perbankan yang lebih aman dan terpercaya di era digital.

KAJIAN TEORI

Penelitian ini menggunakan Teori Perlindungan Konsumen sebagai dasar untuk menganalisis tanggung jawab hukum bank terkait kebocoran data nasabah. Teori ini relevan karena nasabah sebagai konsumen layanan keuangan memiliki hak atas keamanan data pribadi. Berdasarkan UU Perlindungan Konsumen dan UU Perbankan, terdapat empat prinsip dasar yang digunakan: asas keadilan, yang menekankan perlakuan adil antara bank dan nasabah, termasuk kewajiban bank memberikan informasi yang jelas tentang penggunaan data serta kompensasi jika terjadi kebocoran, selanjutnya asas kemanfaatan, yang mengharuskan bank mengelola data untuk memberikan manfaat maksimal bagi nasabah dengan menerapkan teknologi dan sistem keamanan yang efektif;, selanjutnya asas kepastian hukum, yang menjamin hak dan kewajiban terkait perlindungan data diatur dalam kerangka hukum yang jelas, mencakup standar keamanan dan sanksi bagi pelanggaran, dan terakhir asas keseimbangan, yang mengharmoniskan inovasi layanan dengan keamanan data dan pembagian tanggung jawab secara proporsional. Keempat asas ini membentuk kerangka teoritis untuk menilai tanggung jawab bank dalam mencegah dan menangani kebocoran data nasabah, serta merumuskan rekomendasi guna memperkuat sistem perlindungan data di sektor perbankan Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan tiga pendekatan utama. Pertama, pendekatan perundang-undangan (*statute approach*) digunakan untuk menganalisis regulasi terkait perlindungan data nasabah, termasuk UU Perbankan, UU Perlindungan Data Pribadi, dan peraturan OJK. Kedua, pendekatan konseptual (*conceptual approach*) diterapkan untuk memahami konsep-konsep hukum terkait tanggung jawab bank dan perlindungan data. Ketiga, pendekatan kasus (*case approach*) digunakan untuk menganalisis kasus-kasus kebocoran data yang telah terjadi di sektor perbankan.

HASIL PENELITIAN DAN PEMBAHASAN

1. Ruang Lingkup Tanggung Jawab Hukum Bank

Bank memiliki kewajiban hukum untuk melindungi keamanan dan kerahasiaan data nasabah. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan memberikan perlindungan terhadap dana nasabah, tetapi perlindungan terhadap data nasabah masih memerlukan perhatian yang lebih mendalam.[1] Berikut adalah penjelasan mengenai tiga aspek utama tersebut: tanggung jawab administratif, perdata, dan pidana.

a. Tanggung Jawab Administratif

Tanggung jawab administratif diatur oleh Otoritas Jasa Keuangan (OJK) melalui Peraturan OJK No. 38/POJK.03/2016 mengenai Manajemen Risiko Teknologi Informasi.[2] Peraturan ini mengharuskan bank untuk menerapkan kebijakan keamanan informasi yang ketat dan melakukan pengawasan terhadap sistem pengelolaan data nasabah. Apabila terjadi kebocoran data akibat kelalaian dalam pengelolaan sistem keamanan informasi, OJK berhak memberikan sanksi administratif kepada bank, yang dapat berupa denda, teguran tertulis, atau pembatasan kegiatan usaha.

b. Tanggung Jawab Perdata

Tanggung jawab perdata adalah tanggung jawab hukum yang muncul akibat perbuatan melawan hukum (*onrechtmatige daad*) yang diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata).[3] Pasal ini menyatakan bahwa "setiap tindakan melawan hukum yang mengakibatkan kerugian bagi orang lain, mengharuskan pihak yang menyebabkan kerugian tersebut untuk memberikan ganti rugi." Dalam konteks kebocoran data nasabah, jika bank terbukti lalai dalam menjaga kerahasiaan dan keamanan data nasabah sehingga mengakibatkan kerugian bagi nasabah, maka nasabah dapat mengajukan gugatan perdata terhadap bank.

Contoh kasus yang sering terjadi adalah ketika data nasabah bocor dan digunakan untuk kegiatan penipuan atau penyalahgunaan informasi, nasabah yang dirugikan dapat menuntut bank untuk memberikan ganti rugi atas kerugian materiil dan imateriil yang diderita. Kerugian materiil meliputi kehilangan dana atau akses yang tidak sah ke rekening nasabah, sedangkan kerugian imateriil dapat berupa gangguan privasi dan rasa aman nasabah.

c. Tanggung Jawab Pidana

Selain tanggung jawab perdata, bank juga dapat menghadapi tanggung jawab pidana jika terbukti melanggar hukum yang berkaitan dengan perlindungan data nasabah. Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), terdapat sanksi pidana bagi individu atau pihak yang dengan sengaja atau karena kelalaian membocorkan data pribadi tanpa izin.[4] Pasal 65 UU PDP mengatur bahwa setiap orang atau pihak yang mengakses, mengumpulkan, atau menyebarkan data pribadi tanpa izin dapat dikenakan hukuman penjara dan/atau denda yang signifikan.

Misalnya, jika ada bukti bahwa pegawai bank secara sengaja menjual data nasabah kepada pihak ketiga untuk keuntungan pribadi, maka pegawai tersebut dapat dikenai

---

[1] Alfred Yetno. (2024) Tanggung Jawab Bank Dalam Menjaga Keamanan Dan Kerahasiaan Data Nasabah Perbankan Di Indonesia. *Morality: Jurnal Ilmu Hukum*, 10(1). hlm. 67-76

[2] OJK, *Peraturan OJK No. 38/POJK.03/2016 tentang Manajemen Risiko Teknologi Informasi*, mengatur kewajiban bank dalam mengelola risiko dan melindungi data nasabah dari kebocoran informasi.

[3] Pasal 1365 Kitab Undang-Undang Hukum Perdata Indonesia, mengenai perbuatan melawan hukum yang mengharuskan pihak yang menyebabkan kerugian untuk memberikan ganti rugi.

[4] *Pemerintah Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*

sanksi pidana sesuai ketentuan dalam UU PDP. Bank sebagai institusi juga dapat dikenakan denda jika terbukti gagal mengimplementasikan sistem perlindungan data yang memadai.

2. Mekanisme Perlindungan Data Nasabah

Perlindungan data nasabah merupakan aspek penting dalam menjaga kepercayaan dan integritas di sektor keuangan. Dalam dunia yang semakin digital, pengelolaan data pribadi nasabah harus dilakukan dengan standar keamanan tinggi untuk mencegah penyalahgunaan, pencurian data, dan pelanggaran privasi. Dalam Pasal 40 dari UU No. 10 Tahun 1998 tentang Perbankan ditegaskan bahwa bank memiliki kewajiban untuk menjaga kerahasiaan informasi mengenai nasabahnya, termasuk data simpanan maupun transaksi nasabah. Prinsip kerahasiaan bank ini bertujuan melindungi kepercayaan nasabah terhadap lembaga perbankan.[5] Kewajiban tersebut hanya dapat dikesampingkan dalam keadaan tertentu yang diatur oleh undang-undang, seperti untuk kepentingan perpajakan, penyidikan pidana, atau permintaan pengadilan.[6]

Perlindungan data nasabah dapat dilakukan dengan langkah-langkah berikut. Pertama, Penerapan teknologi keamanan yang merupakan fondasi utama dalam melindungi data nasabah, terutama di sektor perbankan. Berbagai teknologi canggih, seperti enkripsi, *firewall*, dan sistem deteksi intrusi, digunakan untuk menjaga kerahasiaan serta integritas data nasabah yang tersimpan di server.[7] Teknologi ini juga memastikan data tetap aman selama proses transmisi melalui jaringan. Selain itu, bank harus menerapkan autentikasi berlapis untuk meningkatkan perlindungan. Contohnya, penggunaan metode verifikasi biometrik seperti sidik jari atau pengenalan wajah[8] dan penggunaan kode *One-Time Password* (OTP) menjadi langkah wajib untuk memverifikasi identitas pengguna. Penggunaan sistem ini bertujuan untuk memastikan hanya pihak berwenang yang dapat mengakses informasi sensitif. Dengan demikian dapat mengurangi risiko kebocoran atau penyalahgunaan data. Penggunaan teknologi keamanan yang tepat tidak hanya melindungi data nasabah, tetapi juga membangun kepercayaan terhadap layanan perbankan digital yang semakin berkembang di era modern ini.

Kedua, Pengaturan kebijakan internal *yang ketat* juga merupakan aspek penting dalam perlindungan data nasabah. Lembaga keuangan harus menyusun kebijakan yang membatasi akses data hanya kepada karyawan yang memiliki wewenang sesuai tugas dan tanggung jawabnya. Langkah ini memastikan bahwa data sensitif tidak disalahgunakan oleh pihak yang tidak berwenang. Selain itu, pelatihan dan edukasi rutin bagi karyawan tentang pentingnya menjaga kerahasiaan data nasabah menjadi keharusan. Edukasi ini bertujuan untuk meningkatkan kesadaran terhadap risiko keamanan dan meminimalkan potensi pelanggaran akibat kelalaian.[9] Dengan kebijakan internal yang kuat, risiko ancaman dari pihak internal dapat ditekan secara signifikan.

Ketiga, kepatuhan terhadap regulasi menjadi kewajiban yang tidak dapat diabaikan oleh lembaga keuangan dalam melindungi data nasabah. Di Indonesia, sejumlah peraturan menjadi landasan hukum utama. Salah satunya Undang-Undang Nomor 27 Tahun 2022 tentang

---

[5] Ferdinan Tambing,dkk. Keamanan Data Nasabah di Bank dan Perlindungan Otoritas Jasa Keuangan. 2023. *Journal Sultra Research of Law*, 5 (1). hal 32

[6] Pasal 2 ayat (2) Peraturan Bank Indonesia Nomor 2/19/PBI/2000 tentang Persyaratan dan Tata Cara Pemberian Perintah Izin Tertulis Membuka Rahasia Bank

[7] Danurdhara Suluh Prasasta. Encryption: Fondasi Utama dalam Operasi Perbankan. Dilansir dari *Mega buana Teknologi*

[8] Biometrik dalam Perbankan: Apa Saja Keuntungan Teknologi Biometrik Bagi Bank?. 2023. Dilansir dari *IProov* https://www.iproov.com/id/blog/biometrics-in-banking-advantages

[9] Kadek Rima Anggen Suari & I Made Sarjana. Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. 2023. *Jurnal Analisis Hukum*.

Perlindungan Data Pribadi (UU PDP) yang mengatur prinsip-prinsip pengelolaan data seperti keharusan memperoleh persetujuan eksplisit dari pemilik data sebelum pengolahan dilakukan dan memastikan hak pemilik data termasuk pada hak untuk mengakses, memperbarui, dan menghapus data pribadi mereka. Selain itu POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan yang mengatur mengenai transparansi, kerahasiaan data, dan mekanisme pengaduan. Regulasi ini dirancang untuk menjaga kepercayaan nasabah serta memastikan pengelolaan data dilakukan sesuai standar hukum yang berlaku.

Keempat, penerapan transparansi dan tanggung jawab memperkuat kepercayaan nasabah. Lembaga keuangan harus memberikan informasi yang jelas mengenai cara data nasabah dikelola dan tujuan penggunaannya.[10] Jika terjadi kebocoran data, bank wajib memberikan notifikasi kepada nasabah yang terdampak serta melaporkan insiden tersebut kepada Otoritas Jasa Keuangan (OJK) dalam waktu 24 jam sesuai ketentuan regulasi. Prosedur ini penting untuk menjaga transparansi dan meminimalkan dampak yang mungkin timbul. Selain itu, bank harus memiliki protokol penanganan insiden yang komprehensif dan rencana pemulihan yang jelas, mencakup langkah-langkah pemulihan data, penyelidikan forensik, serta tindakan pencegahan untuk mencegah kejadian serupa di masa mendatang. Implementasi langkah-langkah ini menunjukkan komitmen bank dalam menjaga kepercayaan nasabah dan mematuhi regulasi yang berlaku.

3. Studi Kasus Kebocoran Data Bank

a. Analisis Kasus Domestik

Kasus kebocoran data yang terjadi pada Bank Indonesia di bulan Desember 2021 menunjukkan pola serangan yang umum terjadi di sektor perbankan, dimana peretas berhasil mengakses dan mencuri data sensitif nasabah melalui celah keamanan sistem. Dalam kasus ini, kelompok peretas bernama BlueNoroff diduga telah mencuri dan memperdagangkan data sensitif dari Bank Indonesia di forum *dark web*.[11] Penanganan kasus oleh Bank Indonesia dan Otoritas Jasa Keuangan (OJK) dilakukan melalui serangkaian langkah cepat, termasuk pembentukan tim investigasi khusus dan peningkatan pengawasan sistem. Bank Indonesia juga segera melakukan audit menyeluruh terhadap infrastruktur teknologi informasi mereka serta memperkuat protokol keamanan data. Dari kasus-kasus serupa yang pernah terjadi sebelumnya di Indonesia, pembelajaran utama yang dapat diambil adalah pentingnya implementasi sistem deteksi dini, backup data yang teratur, serta pelatihan keamanan siber yang berkelanjutan bagi seluruh karyawan.

b. Perbandingan dengan Kasus Internasional

Kasus kebocoran data *First American Financial Corporation* yang terjadi pada Mei 2019 menjadi contoh signifikan dalam konteks keamanan data finansial global. Perusahaan ini mengalami kebocoran yang mengekspos lebih dari 885 juta catatan sensitif nasabah termasuk nomor rekening bank, pernyataan pajak, nomor jaminan sosial, dan data transaksi *real estate* yang dapat diakses secara publik melalui website perusahaan. Kelemahan sistem yang ditemukan berupa kesalahan desain *website* yang memungkinkan akses ke dokumen sensitif hanya dengan memodifikasi digit pada URL. Penanganan kasus ini menjadi pembelajaran penting dimana *Securities and Exchange*

[10] Fajar Dharma Saputra & Rahmi zubaedah. Eksplorasi Kebutuhan Dan Harapan Debitur Terhadap Perlindungan Data Pribadi Dalam Industri Keuangan. 2023. *Jurnal Ilmiah Wahana Pendidikan*, 9 (14).

[11] Anderson, R., & Moore, T. (2021). "Information Security Economics – and Beyond". Proceedings of the International Conference on Financial Cryptography.

Commission (SEC) AS memberikan denda sebesar 487.616 dolar AS kepada *First American* karena dinilai memiliki kelemahan dalam kontrol keamanan *cybersecurity*. [12] Kasus ini juga mendorong penguatan standar internasional untuk keamanan data di sektor finansial, terutama dalam hal enkripsi data sensitif, pengujian keamanan sistem secara berkala, dan implementasi kontrol akses yang lebih ketat.

4. Rekomendasi Penguatan Sistem

a. Aspek Regulasi

Menghadapi ancaman siber yang semakin kompleks, diperlukan pembaruan regulasi yang mampu mengikuti perkembangan teknologi terkini. Regulasi yang ada perlu diperkuat dengan mencakup aspek-aspek baru seperti penggunaan teknologi *blockchain* dan kecerdasan buatan dalam sistem perbankan. Penguatan sanksi hukum juga menjadi prioritas, dengan menerapkan denda yang lebih besar dan konsekuensi pidana yang lebih tegas bagi pelaku kejahatan siber di sektor perbankan. Harmonisasi regulasi antara berbagai lembaga terkait seperti OJK, Bank Indonesia, dan Kementerian Komunikasi dan Informatika juga penting untuk menciptakan kerangka hukum yang komprehensif dan efektif dalam melindungi data perbankan.

b. Aspek Teknis

Dari sisi teknis, peningkatan standar keamanan sistem perlu dilakukan melalui implementasi teknologi enkripsi terbaru, sistem autentikasi berlapis, dan pemantauan aktivitas mencurigakan secara *real-time*. Investasi dalam teknologi pengamanan data harus mencakup pengembangan sistem deteksi intrusi yang lebih canggih, penggunaan *artificial intelligence* untuk mendeteksi anomali, serta implementasi *blockchain* untuk meningkatkan transparansi dan keamanan transaksi. Kerjasama dengan pihak keamanan siber, baik dari sektor swasta maupun pemerintah, perlu diperkuat melalui pembentukan tim respons cepat bersama dan berbagi informasi mengenai ancaman siber terkini. Program pelatihan dan sertifikasi keamanan siber bagi personel IT juga perlu ditingkatkan untuk memastikan kesiapan dalam menghadapi berbagai bentuk ancaman siber.

KESIMPULAN

Penelitian ini mengungkapkan bahwa tanggung jawab hukum bank dalam kasus kebocoran data nasabah bersifat kompleks dan berlapis, mencakup aspek administratif, perdata, dan pidana. Hasil analisis menunjukkan bahwa meskipun telah ada kerangka hukum yang mengatur perlindungan data nasabah, implementasinya masih menghadapi tantangan signifikan akibat pesatnya perkembangan teknologi dan semakin canggihnya ancaman siber. Studi kasus yang dilakukan mengungkapkan bahwa kebocoran data sering terjadi akibat kombinasi kelemahan sistem keamanan dan faktor human error, yang menggarisbawahi pentingnya pendekatan komprehensif dalam perlindungan data. Untuk memperkuat sistem perlindungan data nasabah, diperlukan pembaruan regulasi yang lebih responsif terhadap perkembangan teknologi, peningkatan standar keamanan teknis, dan penguatan kapasitas sumber daya manusia di sektor perbankan. Harmonisasi regulasi antar lembaga terkait dan kerjasama internasional dalam penanganan kejahatan siber juga menjadi faktor krusial dalam membangun sistem perlindungan data yang lebih efektif dan terpercaya di era digital.

[12] Securities and Exchange Commission. (2021). "SEC Charges Title Insurance Company with Cybersecurity Vulnerabilities". SEC Press Release

DAFTAR PUSTAKA

Artikel Jurnal

Anderson, R., & Moore, T. (2021). "Information Security Economics – and Beyond". Proceedings of the International Conference on Financial Cryptography.

Kumar, V., & Singh, M. (2022). "Analysis of Recent Data Breaches in Banking Sector". *Journal of Information Security*, 13(2), 45-60.

Misah., & Sinta, P. S., & Sudiarni., & Himsar, P. O. (2023). Analisis Hukum Terhadap Perlindungan Data Pribadi Nasabah dalam Layanan Perbankan Digital di Indonesia. *Jurnal Pendidikan Sosial, dan Humaniora*, 3(3), 285–290.

Fanny, P. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatisawara*, 34(3), 239–249. https://doi.org/10.29303/jtsw.v34i3.218.

Yetno, A. (2024). Tanggung Jawab Bank Dalam Menjaga Keamanan Dan Kerahasiaan Data Nasabah Perbankan Di Indonesia. *Morality: Jurnal Ilmu Hukum*, 10(1), 67–76. http://dx.doi.org/10.52947/morality.v10i1.424.

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484.

Saputra, F. D., & Zubaedah, R. (2023). Eksplorasi Kebutuhan Dan Harapan Debitur Terhadap Perlindungan Data Pribadi Dalam Industri Keuangan. *Jurnal Ilmiah Wahana Pendidikan*, Juli, 2023(14), 297–306. https://doi.org/10.5281/zenodo.8173498.

Tambing, F., Yusuf, M., Fitriadi, M., & Nadzirin Anshari Nur, M. (2023). Keamanan Data Nasabah di Bank dan Perlindungan Otoritas Jasa Keuangan. *Journal Sultra Research of Law*, *5*(1). https://ojs.pascaunsultra.ac.id/index.php/surel.

Buku Teks

Chaudhary, S. (2020). Handbook of Cyber Security in Financial Services. CRC Press

Newman, L.H. (2021). Digital Security in Banking: A Global Perspective. Springer

Laporan Instansi/Lembaga/Organisasi/Perusahaan

Securities and Exchange Commission. (2021). "SEC Charges Title Insurance Company with Cybersecurity Vulnerabilities". SEC Press Release

Bank Indonesia. (2021). "Laporan Penanganan Insiden Siber 2021". Bank Indonesia Official Report.

Sumber dari internet dengan nama penulis

Danurdhara Suluh Prasasta. (n.d.). *Database Encryption: Fondasi Utama dalam Operasi Perbankan*. Mega Buana Teknologi.

Biometrik dalam Perbankan: Apa Saja Keuntungan Teknologi Biometrik Bagi Bank?. 2023. Dilansir dari IProov

Sumber dari internet tanpa nama penulis (tuliskan nama organisasi/perusahaan)

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM. (2022). Otoritas Jasa Keuangan (OJK).

Hudson Rock. (2021). "Bank Indonesia Data Breach Report". Hudson Rock Threat Intelligence Platform.

Krebs, B. (2019). "First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records". KrebsOnSecurity.

Perundang-Undangan

Pasal 1365 Kitab Undang-Undang Hukum Perdata Indonesia

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Peraturan Bank Indonesia Nomor 2/19/PBI/2000 tentang Persyaratan dan Tata Cara Pemberian Perintah Izin Tertulis Membuka Rahasia Bank

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran

Peraturan OJK Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital

SEC Regulation S-P (17 CFR 248.30), Privacy of Consumer Financial Information and Safeguarding Personal Information