CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

PERLINDUNGAN RAHASIA BANK DI TENGAH PERKEMBANGAN TEKNOLOGI DIGITAL

Nurandini[1], St. Hadijah Wahid[2], Ashari[3], Agustina[4], Olivia Amalia Ramadhani[5], Nur Fauzan Al Buhori[6], Said Agil Padil[7], Resky Awaliyah[8], Ari Sandi[9]
[1-9] Universitas Islam Ahmad Dahlan Sinjai
Jl. Sultan Hasanuddin No. 20, Sinjai
E-mail: agustinaina397@gmail.com

ABSTRAK

Artikel ini mengkaji konsep rahasia bank dan pentingnya dalam konteks kemajuan teknologi digital yang rumit. Dengan metode penelitian literatur, kajian ini menganalisis sumber-sumber seperti literatur, regulasi perbankan, dan dokumen resmi tentang perlindungan data nasabah. Temuan utama menunjukkan bahwa rahasia bank melibatkan aspek hukum, etika, dan ekonomi yang saling terkait untuk menjaga stabilitas dan kepercayaan masyarakat terhadap sistem keuangan. Di era digital, tantangan utama meliputi ancaman siber, pergerakan data yang cepat, keterlibatan pihak eksternal, serta kesalahan manusia dalam melindungi data perbankan. Selain itu, laju perkembangan teknologi yang lebih cepat daripada pembaruan aturan menciptakan celah hukum yang meningkatkan risiko kebocoran data. Kajian ini menekankan bahwa memperkuat rahasia bank memerlukan kolaborasi antara teknologi keamanan, manajemen data, peningkatan kesadaran keamanan, serta regulasi yang fleksibel untuk melindungi nasabah dan stabilitas perbankan.
Kata Kunci: rahasia perbankan, keamanan informasi, perbankan daring, ancaman dunia maya, regulasi keuangan, pelindungan konsumen

ABSTRACT

This article explores the concept of bank secrecy and its urgency amid the complexities of digital technological advancements. Employing a literature review approach, it examines banking regulations, official documents, and scholarly works on customer data protection. Findings reveal that bank secrecy encompasses interconnected legal, ethical, and economic dimensions essential for maintaining public trust and financial system stability. In the digital era, key challenges include cyber threats, rapid data mobility, third-party involvement, and human errors in data safeguarding. Moreover, technology's faster evolution compared to regulatory updates creates legal gaps that heighten data breach risks. The study underscores the need for synergy between security technologies, data governance, enhanced security literacy, and adaptive regulations to ensure customer protection and banking industry stability.
***Kata Kunci**: bank secrecy, information security, online banking, cyber threats, financial regulations, consumer protection*

Article History
Received: Januari 2026
Reviewed: Januari 2026
Published: Januari 2026

Copyright : Author
Publish by : CAUSA

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

CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

PENDAHULUAN

Perkembangan teknologi digital telah mengubah cara manusia mengakses informasi, melakukan transaksi, dan berinteraksi dengan lembaga keuangan(Edman, 2000). Arus informasi kini mengalir dengan sangat cepat dan terbuka, menciptakan ekosistem digital yang efisien sekaligus rentan terhadap berbagai ancaman(Agustin, 2024). Keterhubungan antarplatform digital menjadikan data sebagai aset krusial yang selalu berpindah, tersimpan, dan diproses dalam berbagai sistem secara otomatis(Astuti et al., 2025). Dalam konteks inilah isu mengenai keamanan informasi menjadi semakin mengemuka.

Di tengah transformasi tersebut, sektor perbankan menjadi salah satu pusat aktivitas data paling sensitif. Bank tidak hanya menyimpan dana masyarakat, tetapi juga mengelola informasi pribadi, riwayat transaksi, hingga profil risiko nasabah. Kepercayaan publik terhadap lembaga perbankan bergantung pada kemampuan bank melindungi data tersebut dari kebocoran, penyalahgunaan, maupun ancaman serangan siber. Oleh karena itu, menjaga kerahasiaan data nasabah merupakan kewajiban fundamental yang tidak dapat dinegosiasikan(Kholis, 2024).

Konsep rahasia bank hadir sebagai pilar utama dalam menjaga privasi dan keamanan informasi keuangan. Rahasia bank menuntut lembaga perbankan untuk menjaga seluruh data dan aktivitas keuangan nasabah agar tidak diakses atau disebarluaskan oleh pihak yang tidak berwenang. Di era digital, urgensi penerapan rahasia bank semakin tinggi karena meningkatnya risiko kebocoran informasi melalui teknologi digital, baik akibat kesalahan sistem, kelalaian manusia, maupun serangan siber yang semakin canggih(Zahro et al., 2024).

Dengan demikian, pembahasan mengenai "Menjaga Tirai Informasi, Konsep dan Urgensi Rahasia Bank di Era Digital" menjadi sangat relevan untuk dikaji. Pendahuluan ini mengarahkan fokus pada pentingnya menjaga keamanan data perbankan di tengah derasnya arus digitalisasi, serta bagaimana prinsip rahasia bank harus terus diperkuat untuk melindungi kepentingan nasabah dan menjaga kepercayaan publik terhadap sistem keuangan nasional.

METODE

Jenis Penelitian

Penelitian ini menggunakan metode penelitian kepustakaan (library research), yaitu penelitian yang dilakukan dengan menelaah berbagai literatur dan dokumen yang relevan. Sumber yang digunakan meliputi buku-buku perbankan, artikel jurnal, peraturan perundang-undangan, serta publikasi resmi terkait rahasia bank dan keamanan data di era digital. Melalui analisis literatur tersebut, penelitian ini berupaya memahami konsep, urgensi, serta tantangan penerapan rahasia bank dalam lingkungan perbankan digital.

Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah analisis deskriptif kualitatif. Analisis ini dilakukan dengan menelaah, mengorganisasi, dan menginterpretasikan berbagai sumber literatur seperti buku, jurnal ilmiah, peraturan perbankan, serta dokumen resmi terkait rahasia bank dan keamanan data di era digital. Setiap informasi yang diperoleh diklasifikasikan berdasarkan tema tertentu, kemudian dianalisis untuk menggambarkan konsep rahasia bank, urgensinya dalam perlindungan data nasabah, serta tantangan implementasinya di tengah perkembangan teknologi digital.

Melalui pendekatan ini, penelitian menghasilkan pemahaman yang sistematis dan menyeluruh tanpa menggunakan perhitungan statistik, tetapi berfokus pada pendalaman makna dan keterkaitan antar konsep dalam literatur.

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

HASIL DAN PEMBAHASAN

Konsep Rahasia Bank dalam Perspektif Sistem Keuangan Modern

Dalam sistem keuangan modern, rahasia bank menempati posisi sentral sebagai salah satu pilar yang menopang keberlanjutan industri perbankan. Rahasia bank tidak hanya dipahami sebagai upaya menjaga privasi informasi nasabah, tetapi juga merupakan komponen krusial dalam menciptakan kepercayaan publik, stabilitas ekonomi, serta perlindungan terhadap risiko kejahatan finansial(Sugeng, 2020). Kajian pustaka menunjukkan bahwa rahasia bank berkembang menjadi konsep multidimensi yang melibatkan aspek hukum, etis, ekonomi, dan keamanan digital.

1. Pengertian Rahasia Bank dalam Konteks Berbasis Sistem

Pada awalnya, rahasia bank hanya berkaitan dengan kewajiban bank untuk tidak membuka informasi pribadi nasabah termasuk identitas, rekening, dan segala transaksi terkait. Namun dalam konteks sistem keuangan modern yang semakin digital, konsep ini berkembang menjadi kewajiban institusional untuk melindungi setiap bentuk data keuangan melalui kombinasi tata kelola, regulasi, teknologi, dan kebijakan internal(Dapurahayu et al., 2025).

Rahasia bank kini dipandang sebagai perisai informasi (information shield) yang berfungsi mengamankan data nasabah dari berbagai bentuk ancaman seperti penyalahgunaan identitas, pencurian dana, transaksi ilegal, manipulasi keuangan, hingga penyebaran data secara tidak sah (Balaka et al., 2024).

2. Tiga Dimensi Utama Rahasia Bank

Literatur akademik menguraikan bahwa rahasia bank terdiri dari tiga dimensi yang saling melengkapi dan memiliki implikasi yang berbeda dalam praktiknya:

a. Dimensi Legal

Dimensi legal menekankan bahwa rahasia bank merupakan kewajiban hukum yang bersumber dari undang-undang, peraturan perbankan, serta otoritas pengawas keuangan. Aturan tersebut mengatur Jenis informasi yang dikategorikan sebagai rahasia bank, pihak yang berwenang untuk meminta akses, batasan dan prosedur pembukaan rahasia bank, konsekuensi hukum bagi pelanggaran, baik administratif maupun pidana(Katiandagho et al., 2023).

Di banyak negara termasuk Indonesia, aturan rahasia bank mengalami reformasi untuk menyesuaikan dengan tantangan global seperti pencucian uang, pendanaan terorisme, dan kejahatan lintas negara. Perkembangan ini menunjukkan bahwa rahasia bank sudah bukan lagi prinsip absolut, melainkan prinsip relatif yang dapat dibuka secara terbatas demi kepentingan hukum, investigasi, serta stabilitas sistem keuangan(Sulfiarini et al., 2024).

b. Dimensi Etis

Dimensi etis mencerminkan nilai moral dan profesionalitas perbankan. Bank bertanggung jawab menjaga kerahasiaan nasabah sebagai bagian dari komitmen integritas dan kepercayaan yang menjadi fondasi hubungan antara bank dan masyarakat(Asril, 2018).

Prinsip etis ini mengatur bahwa informasi nasabah tidak boleh digunakan untuk keuntungan pribadi pegawai bank, tidak boleh dibagikan tanpa izin atau alasan yang sah,ank wajib menjamin bahwa seluruh pegawainya memahami dan mematuhi kode etik kerahasiaan data(INDONESIA, n.d.).

Pada era digital, dimensi etis menjadi semakin penting karena perilaku pegawai yang lalai atau tidak etis dapat menyebabkan kebocoran data yang berdampak luas secara ekonomi dan reputasi(Firdausy, 2024).

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

c. Dimensi Ekonomi

Dari perspektif ekonomi, kepercayaan publik adalah aset paling berharga bagi industri perbankan. Tanpa kepercayaan, nasabah enggan menyimpan dana, melakukan investasi, atau menggunakan layanan digital bank. Rahasia bank berfungsi menciptakan rasa aman bahwa dana dan informasi nasabah berada di bawah perlindungan yang kuat(Wijayani, 2017).

Beberapa literatur mengaitkan rahasia bank dengan stabilitas ekonomi makro yaitu kebocoran data dapat memicu penarikan dana besar-besaran (bank run), melemahkan reputasi industri keuangan, mengganggu fungsi intermediasi bank terhadap perekonomian, menurunkan partisipasi masyarakat dalam layanan keuangan formal(Situmorang et al., 2024).

Dengan demikian, dimensi ekonomi rahasia bank berkaitan erat dengan keberlanjutan sistem keuangan secara keseluruhan.

3. Perkembangan Rahasia Bank dalam Tuntutan Global

Analisis pustaka menunjukkan bahwa konsep rahasia bank tidak bersifat statis. Ada pergeseran paradigma yang signifikan:

a. Di era tradisional, rahasia bank bersifat sangat ketat dan hampir absolut dan akses informasi nasabah hanya dimiliki bank dan individu yang diberi kuasa(Asril, 2018).
b. Di era modern dan globalisasi, rahasia bank tetap dijaga, tetapi diberi pengecualian demi kepentingan publik yang lebih besar.
Contoh pengecualian global yaitu seperti, pencegahan pencucian uang (AML), pemberantasan pendanaan terorisme (CFT), pengungkapan pajak lintas negara, investigasi tindak pidana ekonomi.

Komitmen global seperti FATF (Financial Action Task Force) dan kerja sama pertukaran data lintas negara mendorong bank untuk menyeimbangkan antara perlindungan privasi dan transparansi.

Urgensi Rahasia Bank di Era Digital

Perkembangan teknologi digital dalam industri perbankan telah membawa transformasi besar-besaran dalam cara lembaga keuangan mengelola informasi. Digitalisasi membuka peluang efisiensi, kecepatan layanan, dan integrasi sistem keuangan global. Namun, transformasi ini juga mengubah lanskap risiko yang dihadapi bank, terutama dalam hal perlindungan data dan keamanan informasi nasabah. Literatur-literatur modern menunjukkan bahwa rahasia bank tidak pernah sepenting saat ini. Di era digital, kebocoran data bukan hanya masalah teknis, tetapi dapat menjadi ancaman finansial, hukum, sosial, dan reputasional(Maulana, 2021). Urgensi tersebut dapat dipahami melalui empat aspek besar berikut ini:

1. Volume dan Kompleksitas Data Digital

Digitalisasi menyebabkan data perbankan berkembang secara eksponensial. Bank tidak hanya menyimpan data dasar seperti identitas dan saldo, tetapi juga riwayat transaksi harian, jejak digital (digital footprint), data perilaku pengguna, log aktivitas perbankan online, informasi biometrik (fingerprint, face recognition), integrasi dengan platform fintech dan e-commerce(Tambunan & Nasution, 2022).

Dengan besarnya volume dan kompleksitas data tersebut, bank menghadapi tantangan baru, yaitu bagaimana memetakan risiko informasi dalam jaringan yang terbuka dan saling terhubung. Literasi keamanan juga menjadi lebih rumit karena data tidak hanya “disimpan”, tetapi terus bergerak dan diperbarui(Dapurahayu et al., 2025).

Kebocoran pada satu bagian dapat memicu *domino effect* misalnya, kebocoran email nasabah dapat menyebabkan akses ke mobile banking, lalu berlanjut ke

transaksi ilegal. Karena itu, rahasia bank tidak lagi sekadar menjaga informasi finansial, tetapi juga data digital yang menjadi bagian dari identitas elektronik seseorang (*digital identity*).

2. **Meningkatnya Ancaman Siber**

Seiring semakin digitalnya industri keuangan, ancaman siber juga mengalami evolusi. Serangan tidak hanya dilakukan oleh peretas individu, tetapi juga organisasi kriminal internasional, operator di pasar gelap data, kelompok terorganisir yang memanfaatkan kecerdasan buatan, insider threats dari pihak internal bank(Damayanti & Budiono, 2024).

Ancaman seperti *phishing, man-in-the-middle attack, malware, SIM swap fraud*, dan *credential stuffing* menjadi semakin umum. Data perbankan menjadi komoditas yang sangat berharga di *dark web* karena dapat digunakan untuk pencurian dana, pemerasan (*extortion*), penyalahgunaan identitas, pembiayaan tindak pidana (*fraud, money laundering*)(Gulo et al., 2021).

Dengan demikian, urgensi rahasia bank meningkat karena potensi kerugian tidak lagi terbatas pada satu nasabah, tetapi bisa menyasar ribuan bahkan jutaan nasabah sekaligus melalui satu serangan siber skala besar. Bank harus meningkatkan pertahanan digitalnya dengan lapisan keamanan berstandar global.

3. **Mobilitas Data yang Tinggi**

Jika pada era sebelum digital data nasabah disimpan secara terisolasi di bank, maka kini data tersebut bergerak melalui berbagai entitas dan kanal. Mobilitas data terjadi karena sistem interoperabilitas antarbank, kerja sama dengan fintech (open API), platform pembayaran digital (QRIS, switching companies), lembaga verifikasi identitas (e KYC), penggunaan cloud computing, integrasi dengan layanan pihak ketiga (third party providers)(Muqorobin et al., 2021).

Setiap pergerakan data menjadi titik potensi kebocoran. Semakin banyak pihak yang terlibat, semakin sulit bank menegakkan kerahasiaan secara absolut. Inilah alasan mengapa literatur modern menekankan konsep data governance dan risk ownership di mana bank harus mengelola setiap titik risiko secara menyeluruh(Harahap, 2025).

Mobilitas data juga membuat tindakan pengamanan tidak cukup hanya pada tahap penyimpanan. Perlindungan harus mencakup proses transmisi data (enkripsi), proses autentikasi, monitoring aktivitas, audit penggunaan data, evaluasi pihak-pihak eksternal(Harahap, 2025).

Dengan demikian, urgensi penegakan rahasia bank meningkat karena data tidak lagi berada pada satu kontrol terpusat, tetapi pada ekosistem digital yang luas.

Implementasi Rahasia Bank di Era Digital

Implementasi rahasia bank pada era digital tidak lagi hanya berkaitan dengan penyimpanan data, tetapi mencakup perlindungan, pengelolaan, dan pemantauan alur informasi dalam ekosistem yang saling terhubung. Digitalisasi memperluas permukaan risiko (risk surface) sehingga bank harus menghadapi tantangan yang lebih kompleks dibanding era sebelumnya(Harahap, 2025). Hasil kajian pustaka menunjukkan bahwa tantangan tersebut mencakup aspek teknologi, hubungan bisnis, sumber daya manusia, dan kerangka regulasi.

1. **Ancaman Teknologi dan Keamanan Siber**

Era digital memperkenalkan berbagai bentuk ancaman teknis yang semakin canggih dan sulit dideteksi. Serangan tidak hanya berupa pencurian data, tetapi juga manipulasi sistem, penghentian layanan, dan pengendalian jarak jauh(Ali et al., 2025). Bentuk ancaman teknologi meliputi:

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 3 Tahun 2026
Prefix doi.org/10.3783/causa.v2i9.2461

a. Hacking, Malware, dan Ransomware

Peretas dapat menyusup melalui sistem yang lemah atau belum diperbarui (outdated system). Malware modern mampu, mencuri kredensial login, mencatat aktivitas pengguna (keylogging), mengenkripsi seluruh data bank dan meminta tebusan (ransomware), menyalin data sensitif secara diam-diam (data exfiltration)(Serius et al., 2024).

Serangan seperti ini sering memengaruhi seluruh operasi perbankan dan dapat melumpuhkan layanan publik.

b. Penyusupan Sistem (Cyber Intrusion)

Serangan ini memanfaatkan celah keamanan pada server, jaringan, atau aplikasi perbankan. Penyusup dapat, mengubah data nasabah, mengintervensi proses transaksi, memasang backdoor untuk akses jangka panjang(Khoiriah et al., 2025).

Intrusi semacam ini sangat berbahaya karena sulit terdeteksi dan dapat berlangsung bertahun-tahun.

c. Penyalahgunaan API Perbankan

Dalam era open banking, bank banyak membuka API untuk, fintech, startup pembayaran, integrasi e-commerce, platform digital lainnya.

API yang tidak aman dapat dieksploitasi untuk mengambil data nasabah secara masif. Literatur menyebut bahwa API menjadi salah satu titik paling rawan dalam ekosistem keuangan digital(Hossain & Rahman, 2025).

d. Pencurian Data pada Jaringan Tidak Aman

Serangan seperti sniffing, man-in-the-middle attack, atau eksploitasi Wi-Fi publik dapat digunakan untuk mencuri, data login, informasi transaksi, identitas nasabah(Pangestu et al., 2022).

Karena itu, bank perlu memperkuat enkripsi dan menerapkan protokol keamanan tingkat tinggi (TLS, multi-factor authentication).

e. Biaya Keamanan yang Tinggi dan Pembaruan Berkelanjutan

Teknologi berkembang sangat cepat. Sistem keamanan yang relevan hari ini bisa menjadi usang dalam hitungan bulan. Bank wajib melakukan, pembaruan software (*patching*), penilaian kerentanan (*vulnerability assessment*), simulasi serangan (*penetration testing*), peningkatan kapasitas tim keamanan(Al-fadl et al., 2025).

Hal ini menuntut biaya yang sangat besar serta sumber daya manusia yang kompeten, yang tidak semua bank mampu memenuhinya.

2. Keterlibatan Pihak Ketiga (Third Party Risk)

Ekosistem digital membuat bank tidak lagi beroperasi secara mandiri. Bank kini terhubung dengan banyak pihak eksternal, seperti, perusahaan fintech, penyedia cloud computing, penyedia layanan verifikasi biometrik, perusahaan switching, lembaga kliring nasional dan internasional, vendor outsourcing IT, mitra pembayaran digital(Priski & Asiyanti, 2024).

Kerja sama ini meningkatkan efisiensi layanan tetapi memperluas risiko kebocoran data. Tantangan yang muncul antara lain:

a. Standar keamanan yang tidak merata, tidak semua mitra memiliki sistem keamanan yang setara dengan standar perbankan. Jika pihak ketiga lemah, maka seluruh ekosistem ikut terancam.
b. Kurangnya kontrol bank, bank tidak dapat mengawasi seluruh aktivitas teknis pihak ketiga, terutama jika mereka beroperasi di luar negeri atau memiliki sistem internal yang kompleks.

c. Ketergantungan pada outsourcing, beberapa bank sangat bergantung pada pihak eksternal untuk manajemen server, penyimpanan cloud, atau pengembangan aplikasi. Ketergantungan ini meningkatkan risiko jika terjadi, konflik kepentingan, insiden keamanan, penyalahgunaan akses (privileged access).
d. Risiko rantai pasokan (supply chain risk), perusahaan pihak ketiga mungkin juga bekerja sama dengan pihak lain (fourth parties), sehingga jalur data menjadi semakin panjang dan rentan(Faizal et al., 2023).

3. Human Error sebagai Faktor Utama Kebocoran

Literatur keamanan informasi menunjukkan bahwa lebih dari 60% kebocoran data di sektor keuangan berasal dari kesalahan manusia, bukan serangan siber langsung. Hal ini menjadikan human error sebagai tantangan terbesar. Bentuk human error meliputi:

a. Pegawai membagikan informasi secara tidak sengaja, misalnya melalui email, pesan singkat, atau platform tidak resmi tanpa perlindungan.
b. Akses tidak sah oleh pegawai (insider threat), beberapa insiden menunjukkan bahwa pegawai dapat menyalahgunakan akses untuk, menjual data nasabah, membuka informasi untuk kepentingan pihak tertentu, mengakses data di luar kewenangannya.
c. Rendahnya literasi keamanan digital, pegawai mungkin, menggunakan password yang lemah, membuka tautan phishing, tidak mengenali manipulasi sosial (social engineering).
d. Kelalaian dalam mengelola system, seperti gagal memperbarui perangkat lunak, salah konfigurasi server, atau tidak mengaktifkan enkripsi.

4. Regulasi yang Belum Selaras dengan Perkembangan Teknologi

Salah satu tantangan struktural dalam menjaga rahasia bank adalah ketidaksesuaian antara, kecepatan perkembangan teknologi, dan lambatnya penyusunan regulasi. Digitalisasi menghasilkan inovasi yang sangat cepat seperti, open banking, artificial intelligence, blockchain, biometric authentication, cloud computing. Namun, regulasi sering tidak mampu mengimbangi kecepatan tersebut(Zahra et al., 2024). Implikasi ketidaksesuaian regulasi:

a. Adanya area abu-abu (grey area), beberapa layanan finansial baru tidak memiliki aturan teknis yang jelas, sehingga membuka ruang penyalahgunaan atau praktik yang merugikan nasabah(Fred, n.d.).
b. Ketidakpastian Hukum, bank sering menghadapi dilema antara, menaati aturan rahasia bank yang ketat, dan memenuhi kewajiban pelaporan pada otoritas (AML, fraud detection). Tanpa kejelasan hukum, bank dapat salah langkah dan justru melanggar ketentuan(Zahra et al., 2024).
c. Perbedaan standar regulasi antarnegara, dalam transaksi internasional, bank harus menyesuaikan diri dengan regulasi global yang mungkin berbeda dari aturan nasional(Zahra et al., 2024).
d. Keterlambatan pembaruan regulasi, perubahan aturan perbankan sering memakan waktu lama, sementara ancaman digital berkembang lebih cepat. Hal ini menuntut bank dan regulator untuk menjalin kerja sama yang lebih intensif dalam menciptakan regulasi adaptif dan responsif terhadap inovasi digital(Yolanda et al., 2024).

KESIMPULAN

Pembahasan ini menekankan bahwa kerahasiaan perbankan merupakan dasar utama untuk mempertahankan kepercayaan masyarakat, stabilitas finansial, serta perlindungan data pelanggan di zaman digital. Dalam dunia perbankan kontemporer, kerahasiaan ini tidak hanya

memiliki aspek hukum, tetapi juga dimensi moral dan ekonomi yang secara langsung memengaruhi kelangsungan sektor perbankan.

Transformasi digital menjadikan kerahasiaan perbankan semakin krusial akibat peningkatan volume data, kerumitan sistem, pergerakan informasi, serta ancaman keamanan siber yang semakin maju. Situasi ini membuat kebocoran data tidak lagi sekadar masalah kecil, melainkan bisa menyebabkan kerugian ekonomi, kerusakan citra, bahkan bahaya sistemik bagi ketahanan perbankan.

Meski demikian, penerapan kerahasiaan perbankan dihadapkan pada hambatan serius seperti ancaman teknologi, risiko dari pihak eksternal, kesalahan manusia, serta aturan yang sering kali ketinggalan dari kemajuan teknologi. Karena itu, penguatan kerahasiaan perbankan membutuhkan kerja sama antara teknologi keamanan terkini, pengelolaan data yang efektif, peningkatan kesadaran keamanan, dan regulasi yang fleksibel.

Secara umum, pelindungan kerahasiaan perbankan kian penting di era digital untuk memastikan sistem finansial tetap aman, dapat diandalkan, dan siap menghadapi tantangan perubahan digital yang terus berubah.

DAFTAR PUSTAKA

Agustin, S. (2024). *Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber*. *1*(6), 500–504.

Al-fadl, A. M. A., Ahmed, A., Ibrahim, Y., Mohamed, M., & Eid, Z. (2025). *The Impact of Cybersecurity Spending on the Performance in Egyptian Commercial Banks with A Field Study*. *10*(2), 719–741.

Ali, A., Fitri, A. O., Studi, P., & Syariah, P. (2025). *Jurnal Bersama Ilmu Ekonomi Keamanan Perbankan di Era Digital : Tantangan dan Solusinya*. *1*(2), 154–165. https://doi.org/10.55123/ekonom.v1i2.197

Asril, J. (2018). *RAHASIA BANK DAN PERKEMBANGAN PENGATURANNYA DALAMHUKUM POSITIF*. *2*(1), 237–250.

Astuti, Y., Febriani, O. M., Informasi, J. S., Lampung, B., & Digital, P. (2025). *Implementasi Platform Digital Berbasis Web Untuk Manajemen Aset dan Inventarisasi BPBD Lampung*. *19*(x), 679–689.

Balaka, K. I., Hakim, A. R., & Sulistyany, F. D. (2024). Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital. *Yustitiabelen*.

Damayanti, A., & Budiono, A. (2024). KAJIAN HUKUM DAN REGULASI TERKAIT SERANGAN HACKING PADA PLATFORM DIGITAL DI INDONESIA. *Multidisciplinary Indonesian Center Journal (MICJO)*.

Dapurahayu, S., Jauharah, S. A., Febriansyah, Z., Aristito, A. G., & Sjofjan, L. (2025). Dampak Dalam Penggunaan Transaksi Perbankan Digital. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*.

Edman, R. (ed. al. (2000). *Hukum Perlindungan Konsumen*.

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). *ANALISIS RISIKO TEKNOLOGI INFORMASI PADA BANK SYARIAH : IDENTIFIKASI ANCAMAN DAN TANTANGAN TERKINI*. *5*(2), 87–100.

Firdausy, A. (2024). Perilaku Tidak Etis dan Dampaknya terhadap Kepercayaan Publik: Studi Kasus pada Laporan Keuangan Perusahaan. *Ilmu Ekonomi Manajemen dan Akuntansi*.

Fred, T. (n.d.). *Persimpangan Inovasi Fintech dan Regulasi Keuangan: Perspektif Global*. 34–56.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS*.

Harahap, A. M. (2025). *ANALISIS RISIKO DALAM DIGITALISASI PERBANKAN SYARIAH : TANTANGAN DAN SOLUSI*. *10*(204), 686–705.

Hossain, M. A., & Rahman, J. Y. (2025). *Investigating the Cybersecurity Implications of Open Banking and Application Programming Interfaces (APIs) in the Financial Sector*. *4*(1), 39–56.

INDONESIA, B. B. S. (n.d.). *KODE ETIK (CODE OF CONDUCT) PT BANK SYARIAH INDONESIA Tbk*.

Katiandagho, V., Putong, D. D., & Melo, I. J. (2023). *UNDANG – UNDANG PERLINDUNGAN DATA PRIBADI MEMPERKUAT UNDANG – UNDANG PERBANKAN DALAM MENJAGA RAHASIA DATA NASABAH DAN UNTUK MELINDUNGI DATA PRIBADI MASYARAKAT INDONESIA*. *9*(1), 106–114.

Khoiriah, S., Salsabila, A., Camberra, D. D., Syafri, E., Lina, H., Fathurrahman, R., & Marjohan, M. (2025). *Keamanan dan Privasi dalam Keuangan Digital*. *2023*.

Kholis, I. M. (2024). *Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan : Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia*. *4*(2).

Maulana, A. (2021). *Transformasi Digital*.

Muqorobin, M. M., Anggraini, A., Rahmawati, A. D., Yohanes, D., & Ifkarina, F. D. (2021). Pengaruh Open Banking berbasis Open API terhadap Eksistensi Perbankan. *MAKSIMUM*.

Pangestu, T., Liza, R., Studi, P., Informatika, T., & Medan, U. H. (2022). *ISSN 2338-5677 Cetak ISSN 2548-6646 Online Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing ISSN 2338-5677 Cetak ISSN 2548-6646 Online*. *10*(2), 60–67.

Priski, A., & Asiyanti, D. (2024). *Strategi Manajemen Risiko dan Keamanan Siber dalam Ekonomi Digital : Tinjauan Literatur*.

Serius, A., Era, D., Balaka, K. I., Hakim, A. R., & Sulistyany, F. D. (2024). *Pencurian Informasi Nasabah Di Sektor Perbankan : 10*(3), 105–130.

Situmorang, F., Syahbana, E., & Alisya, J. (2024). *Membangun Kepercayaan Masyarakat Terhadap Bank Syariah : Sebuah Tinjauan Literatur Tentang Strategi dan Tantangan*. *3*.

Sugeng. (2020). *Hukum Telematika Indonesia*.

Sulfiarini, W., Marwiyah, S., Prawesthi, W., & Amiq, B. (2024). *ANALISIS HUKUM TERHADAP PEMBUKAAN RAHASIA BANK TENTANG PENCEGAHAN DAN PEMBERANTASAN TINDAK PIDANA PENCUCIAN UANG*.

Tambunan, R. T., & Nasution, M. I. P. (2022). Tantangan dan Strategi Perbankan Dalam Menghadapi Perkembangan Transformasi Digitalisasi di Era 4.0. *Sci-Tech Journal*.

Wijayani, D. R. (2017). *Kepercayaan Masyarakat Menabung pada Bank Umum Syariah*. *8*(1), 1–12.

Yolanda, E., Lindawaty, P., Sewu, S., Andersen, C., Hukum, F., & Maranatha, U. K. (2024). *Analisis Hukum Tantangan Bank Digital Dihubungkan dengan Perlindungan Hukum Bagi Nasabah Berdasarkan Perundang- Undangan di Indonesia*. *5*(4), 2876–2886.

Zahra, H., Lestari, D. I., & Fahmi, M. H. (2024). *KEPATUHAN HUKUM DALAM OPERASIONAL BANK DIGITAL ,*. *2*(6), 112–122.

Zahro, N., Zahra, I. A., & Faidhah, Y. S. (2024). *Upaya perlindungan hukum terhadap rahasia bank guna menjaga kepentingan nasabah bank*. *2*(6), 38–48.