Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 209-215

Tantangan Hukum dalam Integrasi Sistem Perbankan Digital dan Keamanan Siber di Indonesia

Henri Marusaha Tambunan[1], Devi Noviarani[2], Winda Agustina Damayanti[3]
[123]Fakultas Hukum, Universitas Negeri Semarang
Email: henritambunan3@students.unnes.ac.id[2], devinoviarani@students.unnes.ac.id[2], damayantiw681@students.unnes.ac.d[3]

Abstract
Transformasi digital dalam sektor perbankan Indonesia telah menciptakan berbagai tantangan hukum yang signifikan, terutama dalam aspek keamanan siber dan perlindungan data nasabah. Penelitian ini bertujuan untuk menganalisis kompleksitas tantangan hukum dalam integrasi sistem perbankan digital dan keamanan siber di Indonesia, serta mengidentifikasi solusi yang dapat diterapkan untuk mengatasinya. Metodologi yang digunakan adalah analisis yuridis normatif dengan pendekatan perundang-undangan dan studi kasus. Hasil penelitian menunjukkan bahwa tantangan utama mencakup kepatuhan regulasi, perlindungan data nasabah, jurisdiksi dalam transaksi lintas batas, dan penegakan hukum dalam kejahatan siber. Penelitian ini menemukan bahwa diperlukan penguatan regulasi, peningkatan investasi infrastruktur keamanan, dan pengembangan SDM yang kompeten untuk menghadapi tantangan tersebut. Kesimpulannya, keberhasilan integrasi sistem perbankan digital dan keamanan siber di Indonesia membutuhkan pendekatan komprehensif yang melibatkan kolaborasi antara regulator, industri perbankan, dan pemangku kepentingan lainnya, serta kerangka hukum yang adaptif terhadap perkembangan teknologi.

Article History
Received Okt 17, 2024
Revised Okt 20, 2024
Accepted 29 Okt 2024
Available online 07 Nov. 2024

Keywords :
perbankan digital, keamanan siber, regulasi, perlindungan data, hukum siber

Abstract
The digital transformation in the Indonesian banking sector has created significant legal challenges, especially in terms of cybersecurity and customer data protection. This study aims to analyze the complexity of legal challenges in the integration of digital banking systems and cybersecurity in Indonesia, and to identify solutions that can be applied to overcome them. The methodology used is normative legal analysis with a legislative approach and case studies. The results of the study indicate that the main challenges include regulatory compliance, customer data protection, jurisdiction in cross-border transactions, and law enforcement in cybercrime. This study found that it is necessary to strengthen regulations, increase investment in security infrastructure, and develop competent human resources to face these challenges. In conclusion, the success of the integration of digital banking systems and cybersecurity in Indonesia requires a comprehensive approach that involves collaboration between regulators, the banking industry, and other stakeholders, as well as a legal framework that is adaptive to technological developments.

Keywords :
digital banking, cybersecurity, regulation, data protection, cyber law

https://doi.org/10.5281/zenodo.14068424

PENDAHULUAN

Perbankan berperan sebagai perantara keuangan yang memberikan layanan keuangan kepada masyarakat, seperti memberikan pinjaman, giro, tabungan, investasi, dan penyediaan berbagai produk dan layanan keuangan lainnya. Namun seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi, industri perbankan menghadapi berbagai tantangan baru dalam menjalankan kegiatan usahanya. Era digital telah membawa perubahan signifikan terhadap cara masyarakat melakukan dan berinteraksi dalam transaksi keuangan. Layanan perbankan digital seperti internet banking, mobile banking, dan transaksi elektronik telah menjadi bagian integral dari kehidupan masyarakat sehari-hari. Kehadiran teknologi ini memberikan kemudahan dan kenyamanan kepada nasabah perbankan sehingga dapat mengakses layanan perbankan kapan saja dan dimana saja. Namun, di balik manfaat perbankan digital terdapat tantangan hukum dan risiko yang perlu diatasi.

Mengingat ancaman kejahatan dunia maya dan pelanggaran keamanan informasi, keamanan data dan perlindungan pelanggan menjadi perhatian utama.Selain itu, penipuan elektronik, pencucian uang, dan praktik perbankan yang tidak etis juga merupakan masalah serius yang perlu diatasi.

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 209-215

Perubahan perilaku konsumen juga menjadi faktor penting untuk dipertimbangkan. Pengenalan teknologi digital telah mengubah cara masyarakat melakukan transaksi keuangan, beralih dari penggunaan uang tunai ke pembayaran digital yang semakin populer. Bank perlu memahami dampak perubahan ini terhadap kebijakan moneter, stabilitas harga, dan kesehatan sistem keuangan secara keseluruhan. Hal ini memerlukan analisis terperinci mengenai bagaimana perubahan teknologi kemungkinan besar akan berdampak pada dinamika perekonomian nasional dan global.

Di era digital, regulasi perbankan harus mengikuti perkembangan teknologi dan mengantisipasi tantangan baru. Regulasi yang efektif dan adaptif merupakan kunci untuk menjaga stabilitas sektor perbankan, mengurangi risiko hukum dan meningkatkan kepercayaan nasabah. Perbankan merupakan sektor yang sangat penting dalam perekonomian suatu negara. Di era digitalisasi yang semakin meningkat, industri perbankan menghadapi berbagai tantangan hukum yang unik dan kompleks. Regulasi perbankan yang efektif dan adaptif sangat penting untuk memastikan keamanan, transparansi dan kepercayaan pada sistem perbankan. Oleh karena itu, penelitian ini bertujuan untuk menganalisis peran regulasi yang ada saat ini dalam mengatasi tantangan perbankan di era digital. Masalah yang akan diteliti yaitu apa saja tantangan hukum yang dihadapi oleh industri perbankan di era digital, bagaimana regulasi terkini telah beradaptasi untuk mengatasi tantangan tersebut dan bagaimana dampak perubahan regulasi terhadap aktivitas perbankan di era digita.

METODE PENELITIAN

Penelitian ini dilakukan dengan pendekatan kualitatif yang menggabungkan analisis literatur, pemeriksaan dokumen hukum, serta kajian peraturan perbankan terkini, dengan tujuan untuk memperoleh pemahaman yang mendalam mengenai tantangan hukum yang dihadapi sektor perbankan di Indonesia dalam era digital. Dalam proses penelitian, data dan informasi yang relevan dikumpulkan dari berbagai sumber yang terverifikasi, termasuk jurnal ilmiah, laporan penelitian, peraturan hukum, dan publikasi terkait industri perbankan. Melalui analisis komprehensif, penelitian ini bertujuan untuk menjelaskan peran peraturan yang berlaku saat ini dalam mengatasi tantangan hukum dan risiko yang muncul akibat perkembangan teknologi informasi dan komunikasi. Selain itu, penelitian ini juga berfokus pada identifikasi dan analisis faktor-faktor yang memengaruhi sektor perbankan di Indonesia di tengah perubahan cepat yang dipicu oleh kemajuan siber, sehingga memberikan wawasan yang lebih luas tentang bagaimana industri perbankan dapat beradaptasi dan berkembang dalam konteks yang terus mengalami perubahan ini.

HASIL DAN PEMBAHASAN

Tantangan Hukum dalam Integrasi Sistem Perbankan Digital Terkait Keamanan Siber dan Perlindungan Data Nasabah

Tantangan hukum yang dihadapi industri perbankan di era digital berdampak signifikan terhadap operasional bisnis dan kepercayaan nasabah. Untuk menjawab tantangan tersebut, regulasi perbankan harus mampu mengikuti perkembangan teknologi dan memberikan perlindungan yang memadai kepada seluruh pihak yang terlibat di sektor perbankan. Salah satu tantangan terbesarnya adalah keamanan data dan privasi pelanggan. Risiko keamanan siber semakin meningkat di era digital yang semakin terhubung. Pelanggaran data dan serangan peretas dapat mengakibatkan kerugian finansial yang signifikan bagi pelanggan dan lembaga keuangan. Oleh karena itu, peraturan perbankan harus memastikan bahwa lembaga keuangan menerapkan langkah-langkah keamanan yang tepat seperti enkripsi data, otentikasi yang kuat, dan perlindungan dari serangan dunia maya.

Regulasi perbankan harus mampu mempertimbangkan tren tersebut dengan menjaga keseimbangan antara perlindungan konsumen, inovasi, dan stabilitas sistem keuangan. Kolaborasi antara regulator dan pemangku kepentingan industri perbankan perlu ditingkatkan untuk memastikan regulasi sejalan dengan perkembangan fintech (Tambunan & Anwar, 2019). Mengingat risiko keamanan tersebut, penting untuk memilih penyedia layanan keuangan digital yang andal dengan sistem keamanan yang kuat. Selain itu, Anda perlu meningkatkan pengetahuan keuangan dan pemahaman tentang penggunaan teknologi keuangan sehingga Anda dapat melindungi diri sendiri dan mendapatkan manfaat maksimal. Seiring dengan kemajuan era digital, transformasi keuangan

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 209-215

menjadi hal yang penting bagi masyarakat. Memahami dan menerapkan fintech dapat membantu masyarakat yang sebelumnya tidak memiliki akses terhadap sistem keuangan formal. Komunitas bertindak sebagai jembatan antara teknologi keuangan dan masyarakat, memberikan pendidikan dan akses terhadap layanan keuangan digital.

Oleh karena itu, Peraturan Perbankan memerlukan pengembangan kerangka kerja yang memungkinkan kerja sama antarlembaga dan harmonisasi peraturan di tingkat internasional. Untuk menghadapi tantangan-tantangan ini, regulasi perbankan memerlukan kemampuan yang fleksibel dan beradaptasi terhadap perubahan teknologi dan kebutuhan industri. Regulasi perbankan yang efektif harus mampu melindungi kepentingan nasabah, menjamin keamanan dan stabilitas sistem keuangan, serta merangsang inovasi di sektor perbankan.

Integrasi sistem perbankan digital di Indonesia menghadapi beberapa tantangan hukum yang signifikan. Pertama, aspek keamanan siber yang menjadi perhatian utama mengingat meningkatnya ancaman kejahatan siber. Menurut data Badan Siber dan Sandi Negara (BSSN), sepanjang tahun 2023 terjadi peningkatan 43% kasus serangan siber di sektor perbankan dibandingkan tahun sebelumnya. Bank Indonesia melalui PBI No. 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran telah menetapkan standar keamanan siber, namun implementasinya masih menghadapi kendala teknis dan operasional. Penelitian Sujono dan Waluyo (2023) menunjukkan bahwa 60% bank di Indonesia masih kesulitan memenuhi standar keamanan yang ditetapkan karena keterbatasan infrastruktur dan sumber daya manusia.

Dalam hal perlindungan data nasabah, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan landasan hukum baru. Namun, adanya upaya identifikasi kemudian ditemukan adanya gap antara regulasi dan implementasi di lapangan, terutama dalam aspek:

1. Mekanisme consent management
   Ini merupakan sistem untuk mengelola izin nasabah terkait pengumpulan, penyimpanan, dan pemanfaatan data pribadi mereka. Sistem ini bertujuan memastikan bahwa data digunakan sesuai dengan izin yang diberikan nasabah, serta memberikan fleksibilitas untuk diubah atau dicabut kapan saja. Untuk penerapan yang efektif, diperlukan standar nasional agar prosedur konsisten di seluruh lembaga keuangan.
2. Prosedur penanganan kebocoran data
   Ini adalah serangkaian langkah yang diambil ketika terjadi pelanggaran atau kebocoran data nasabah. Prosedur ini mencakup deteksi awal kebocoran, analisis dampak, pemberitahuan kepada pihak-pihak yang relevan, dan langkah pemulihan untuk mencegah kejadian serupa. Prosedur yang baik juga melibatkan pembentukan tim khusus yang memiliki keahlian di bidang keamanan data.
3. Standar enkripsi data nasabah
   Ini adalah kebijakan yang menetapkan metode untuk mengenkripsi data nasabah agar tetap terlindungi selama penyimpanan dan pengiriman. Standar enkripsi yang memadai mencakup penggunaan teknik enkripsi terbaru dan pembaruan berkala sesuai kemajuan teknologi keamanan. Tujuan utamanya adalah mencegah akses tidak sah ke data nasabah.
4. Protokol transfer data lintas sistem
   Ini adalah aturan mengenai cara pengiriman data nasabah dari satu sistem ke sistem lainnya, terutama saat melibatkan platform berbeda atau pihak ketiga. Protokol ini penting untuk menjaga keamanan dan integritas data selama proses pengiriman serta memastikan bahwa data hanya diakses oleh pihak yang memiliki izin.

Integrasi sistem perbankan digital menghadapi sejumlah tantangan hukum yang penting, terutama terkait dengan keamanan siber dan perlindungan data nasabah. Pertama, kepatuhan terhadap berbagai regulasi yang bervariasi di setiap negara menjadi kompleks, karena bank perlu menyesuaikan sistem mereka dengan berbagai peraturan yang ada, yang tentunya memerlukan sumber daya yang besar. Selain itu, dengan meningkatnya volume data yang dikumpulkan, tantangan dalam melindungi data pribadi dari akses yang tidak sah menjadi sangat penting, mengingat bahwa pelanggaran data dapat berakibat pada sanksi hukum dan kerugian reputasi yang signifikan. Ketidakjelasan mengenai tanggung jawab hukum dalam kasus kebocoran data atau serangan siber juga menyulitkan institusi perbankan untuk menetapkan kebijakan dan prosedur yang tepat.

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 209-215

Kerja sama dengan pihak ketiga, seperti penyedia layanan teknologi, menambah tingkat kompleksitas dalam hal pengawasan dan akuntabilitas, terutama berkenaan dengan perlindungan data dan keamanan informasi. Selain itu, edukasi dan kesadaran di kalangan karyawan dan nasabah menjadi sangat penting, karena kurangnya pemahaman dapat meningkatkan risiko kerentanan. Terakhir, perkembangan ancaman siber yang cepat sering kali melebihi kemampuan hukum dan regulasi untuk mengejarnya, menciptakan celah dalam perlindungan hukum. Oleh karena itu, untuk mengatasi tantangan ini, diperlukan kolaborasi yang kuat antara pihak perbankan, regulator, dan pemangku kepentingan lainnya dalam menciptakan kerangka hukum yang adaptif dan menyeluruh.

Efektivitas Kerangka Hukum dalam Mengatur dan Mengawasi Keamanan Sistem Perbankan Digital di Indonesia

Kerangka hukum dalam sistem perbankan digital Indonesia telah menunjukkan perkembangan yang signifikan, tercermin dari implementasi berbagai regulasi komprehensif termasuk UU Perlindungan Data Pribadi dan regulasi Bank Indonesia. Sistem pengawasan dilaksanakan secara multilevel oleh berbagai institusi seperti BI, OJK, dan BSSN, yang meliputi audit keamanan periodik dan penegakan sanksi bagi pelanggar. Analisis efektivitas kerangka hukum dalam pengaturan dan pengawasan keamanan sistem perbankan digital di Indonesia menunjukkan beberapa aspek penting yang perlu dievaluasi. Menurut penelitian Wijaya dan Santoso (2023), kerangka hukum yang ada masih memiliki celah dalam mengantisipasi perkembangan teknologi perbankan digital. Hal ini terlihat dari beberapa indikator berikut:

Aspek Regulasi dan Implementasi

Kerangka regulasi saat ini diatur dalam beberapa instrumen hukum utama:

- POJK No. 12/POJK.03/2021 tentang Bank Umum
- PBI No. 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran
- UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Dalam sistem perbankan digital Indonesia, koordinasi antar lembaga pengawas melibatkan tiga institusi utama yang memiliki peran berbeda namun saling melengkapi. Bank Indonesia (BI) berperan mengawasi sistem pembayaran dan transaksi digital untuk menjaga stabilitas moneter, termasuk memastikan kepatuhan terhadap regulasi sistem pembayaran dan keamanan transaksi elektronik. Sementara itu, Otoritas Jasa Keuangan (OJK) berkonsentrasi pada pengawasan operasional bank, khususnya dalam aspek manajemen risiko digital dan perlindungan konsumen dalam layanan perbankan digital. Badan Siber dan Sandi Negara (BSSN) memiliki tanggung jawab spesifik dalam mengawasi dan menangani ancaman keamanan siber di sektor perbankan. Ketiga lembaga ini perlu menjalin koordinasi erat melalui sistem pelaporan terpadu, pertemuan koordinasi rutin, dan pembentukan tim gabungan untuk penanganan insiden.

Standarisasi protokol keamanan menjadi aspek krusial dalam menjaga integritas sistem perbankan digital. Hal ini mencakup implementasi enkripsi data dengan standar minimal AES-256 untuk melindungi data nasabah, penerapan autentikasi multi-faktor (MFA) untuk akses sistem dan transaksi, serta penggunaan firewall dan sistem deteksi intrusi (IDS/IPS) yang terstandar. Selain itu, diperlukan protokol backup dan disaster recovery yang seragam, standar keamanan aplikasi mobile banking dan internet banking yang konsisten, serta prosedur verifikasi identitas nasabah yang terstandar untuk memastikan keamanan menyeluruh sistem perbankan digital.

Mekanisme audit keamanan sistem dilaksanakan melalui dua pendekatan utama: audit internal dan eksternal. Audit internal meliputi pemeriksaan berkala sistem keamanan yang dilakukan minimal setiap tiga bulan, evaluasi kepatuhan terhadap standar keamanan, pengujian penetrasi sistem secara rutin, serta pemeriksaan log sistem dan aktivitas mencurigakan. Sementara audit eksternal dilakukan oleh pihak ketiga terakreditasi minimal setahun sekali, mencakup penilaian kerentanan sistem secara menyeluruh, evaluasi kesesuaian dengan regulasi yang berlaku, dan pengujian ketahanan sistem terhadap serangan siber. Hasil audit kemudian ditindaklanjuti melalui pelaporan temuan ke manajemen dan regulator, penyusunan rencana perbaikan dengan timeline yang jelas, implementasi rekomendasi hasil audit, serta evaluasi efektivitas perbaikan yang dilakukan.

Keseluruhan aspek ini saling terintegrasi dan membutuhkan implementasi yang terkoordinasi untuk menciptakan sistem perbankan digital yang aman dan terpercaya. Keberhasilan implementasi

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 209-215

bergantung pada komitmen seluruh pemangku kepentingan dan evaluasi berkala untuk penyempurnaan berkelanjutan. Hal ini sejalan dengan berbagai regulasi yang berlaku, seperti PBI No. 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran dan POJK No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital, serta mengacu pada panduan keamanan siber dari BSSN dan standar nasional teknologi finansial dari Bank Indonesia.

Namun dalam pelaksanaannya, sejumlah tantangan masih perlu dihadapi. Permasalahan utama terletak pada overlapping otoritas antar badan pengawas yang berdampak pada lemahnya koordinasi penanganan masalah. Di samping itu, minimnya sumber daya manusia yang kompeten di sektor teknologi perbankan serta beragamnya standar keamanan antar institusi perbankan menciptakan tantangan tersendiri. Kompleksitas masalah semakin bertambah dengan tingginya biaya penerapan sistem keamanan dan lamanya proses investigasi.

Mengatasi berbagai tantangan ini membutuhkan pendekatan bertahap dan sistematis. Strategi jangka pendek (1 tahun) berfokus pada pembentukan satuan tugas khusus untuk koordinasi pengawasan antar lembaga, standardisasi keamanan fundamental, dan program pelatihan intensif untuk personel pengawas. Dalam periode menengah (2-3 tahun), pengembangan diarahkan pada implementasi sistem monitoring terintegrasi, modernisasi infrastruktur teknologi perbankan, dan peningkatan kapasitas tenaga ahli. Sedangkan rencana jangka panjang (3-5 tahun) mencakup integrasi sistem pengawasan skala nasional, inovasi teknologi perbankan lokal, dan standarisasi sesuai kelas internasional.

Aspek-aspek yang menjadi prioritas meliputi pembentukan lembaga koordinasi terpadu untuk mengeliminasi tumpang tindih, simplifikasi mekanisme pelaporan, peningkatan standar keamanan, pengembangan kompetensi tim pengawas, pembangunan fasilitas infrastruktur kolaboratif, dan implementasi pengawasan real-time. Rangkaian solusi ini diproyeksikan dapat mewujudkan ekosistem perbankan digital yang lebih terjamin keamanannya, responsif dalam penanganan masalah, efektif dalam pengawasan, dan optimal dalam perlindungan nasabah.

Implementasi solusi yang berkelanjutan dan sistematis diharapkan dapat menghadirkan transformasi sistem perbankan digital yang unggul dalam aspek keamanan dan efisiensi, sekaligus meningkatkan tingkat kepercayaan publik. Urgensi ini semakin relevan mengingat posisi strategis perbankan digital sebagai katalis pertumbuhan ekonomi digital Indonesia. Kesuksesan program ini akan sangat ditentukan oleh sinergitas dan dedikasi seluruh pemangku kepentingan, mulai dari otoritas regulasi, lembaga perbankan, hingga sektor industri teknologi.

Solusi untuk Mengatasi Kelemahan

1. Peningkatan Edukasi dan Kesadaran:
- Program Pelatihan Spesifik: Mengadakan pelatihan yang dirancang khusus untuk karyawan bank tentang tren terbaru dalam keamanan siber, termasuk simulasi serangan siber untuk meningkatkan kesiapan.
- Kampanye Kesadaran Publik: Meluncurkan kampanye yang menargetkan nasabah untuk mengenali tanda-tanda penipuan siber dan melindungi informasi pribadi mereka. Misalnya, menggunakan media sosial dan forum komunitas untuk memberikan informasi dan tips tentang keamanan.

2. Pembaruan Regulasi Secara Berkala:
- Mekanisme Review: Menetapkan jadwal tahunan untuk meninjau dan memperbarui regulasi agar selalu relevan dengan cepatnya perubahan teknologi dan ancaman baru.
- Keterlibatan Stakeholder: Mengadakan forum dialog antara regulator, industri, dan akademisi untuk membahas perkembangan terbaru dan tantangan yang dihadapi dalam keamanan siber.

3. Penegakan Hukum yang Lebih Ketat:
- Peningkatan Sanksi: Memperkenalkan sanksi yang lebih berat bagi pelanggaran yang mengakibatkan kerugian signifikan bagi nasabah. Misalnya, denda yang proporsional dengan ukuran lembaga dan dampak pelanggaran.
- Audit Keamanan Rutin: Mengharuskan lembaga keuangan untuk menjalani audit keamanan siber secara berkala oleh pihak ketiga yang independen untuk memastikan kepatuhan terhadap regulasi dan standar keamanan.

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 209-215

4. Meningkatkan Koordinasi Antar Lembaga:
- Pembentukan Tim Tanggap Darurat: Membuat tim lintas lembaga yang dapat segera beraksi saat terjadi insiden siber, dengan protokol yang jelas untuk komunikasi dan tindakan.
- Platform Berbagi Informasi: Membangun platform online untuk berbagi informasi tentang ancaman dan insiden keamanan siber di antara lembaga-lembaga terkait.

5. Pengembangan Standar Keamanan yang Jelas:
- Standar Minimum yang Ditetapkan: Menyusun dan mengumumkan standar minimum untuk keamanan sistem informasi yang harus dipatuhi oleh semua lembaga keuangan.
- Program Sertifikasi Keamanan: Mengembangkan program sertifikasi untuk lembaga yang menunjukkan bahwa mereka telah memenuhi atau melampaui standar yang ditetapkan, memberikan insentif untuk peningkatan berkelanjutan.

Dengan menerapkan langkah-langkah konkret ini, seperti peningkatan edukasi dan kesadaran, pembaruan regulasi secara berkala, serta penegakan hukum yang lebih ketat, diharapkan kerangka hukum yang ada di Indonesia dapat menjadi lebih efektif dalam mengatur dan mengawasi keamanan sistem perbankan digital. Hal ini akan memungkinkan lembaga keuangan untuk beroperasi dengan lebih aman dan transparan, sehingga dapat memberikan perlindungan yang lebih baik bagi nasabah dari berbagai ancaman siber. Selain itu, pendekatan yang komprehensif dan kolaboratif antara regulator, lembaga keuangan, dan pemangku kepentingan lainnya sangat penting untuk menciptakan ekosistem perbankan digital yang aman, terpercaya, dan mampu beradaptasi dengan cepat terhadap perkembangan teknologi dan tantangan baru di masa depan.

SIMPULAN

Berdasarkan analisis komprehensif terhadap tantangan hukum dalam integrasi sistem perbankan digital dan keamanan siber di Indonesia, dapat disimpulkan bahwa masih terdapat berbagai kendala signifikan yang perlu diatasi. Tantangan utama mencakup aspek keamanan siber dan perlindungan data nasabah, implementasi regulasi yang belum optimal, koordinasi antar lembaga pengawas yang masih lemah, serta keterbatasan infrastruktur dan sumber daya manusia. Kerangka hukum yang ada masih menunjukkan beberapa kelemahan, termasuk regulasi yang cenderung reaktif terhadap perkembangan teknologi, sistem pengawasan yang belum terintegrasi secara optimal, serta adanya gap antara regulasi dan implementasi di lapangan. Evaluasi terhadap efektivitas kerangka hukum dalam mengatur dan mengawasi keamanan sistem perbankan digital menunjukkan perlunya penguatan di berbagai aspek. Hal ini terlihat dari masih tingginya angka insiden keamanan siber di sektor perbankan, keterbatasan dalam penegakan hukum, serta belum optimalnya sistem koordinasi antar lembaga pengawas. Kondisi ini menggambarkan bahwa diperlukan pendekatan yang lebih komprehensif dan sistematis dalam mengatasi tantangan keamanan sistem perbankan digital di Indonesia.

REFERENSI

Abubakar, L., & Handayani, T. (2022). Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan Di Era Ekonomi Digital. Masalah-Masalah Hukum,51(3),259-270.

Ardianto, R., Ramdhani, R. F., Dewi, L. O. A., Prabowo, A., Saputri, Y. W., Lestari, A. S., & Hadi, N. (2024). Transformasi Digital dan Antisipasi Perubahan Ekonomi Global dalam Dunia Perbankan. MARAS: Jurnal Penelitian Multidisiplin, 2(1), 80–88.

Adrian Sutedi, S. H. (2023). Hukum Perbankan: Suatu Tinjauan Pencucian Uang, Merger, Likuidasi, dan Kepailitan. Sinar Grafika.

Ahmad, R., & Sutanto, H. (2023). "Analisis Keamanan Sistem Perbankan Digital di Indonesia." Jurnal Sistem Informasi, 15(2), 45-60.

Dewi, S. (2023). "Gap Analysis Implementasi Regulasi Perbankan Digital di Indonesia." Jurnal Hukum Bisnis, 12(1), 78-92.

Pratama, B., & Wijaya, R. (2023). "Tantangan dan Peluang Pengembangan Sistem Perbankan Digital." Jurnal Teknologi Informasi, 8(3), 112-125.

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 209-215

Sujono & Waluyo. (2023). "Evaluasi Standar Keamanan Perbankan Digital di Indonesia." Jurnal Manajemen Teknologi, 10(4), 156-170.
Hermansyah. *"Hukum Perbankan Digital Indonesia"*.(Jakarta: Kencana. (2023)).Hlm 56-59
Kasmir. *"Dasar-Dasar Perbankan Digital"*. (Jakarta: Rajawali Pers.(2023)).Hlm 76-83
Sutedi, A. (2023). *"Aspek Hukum Perbankan Digital"*. (Jakarta: Sinar Grafika.(2023)).Hlm 102-108