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 392-397

Analisis Tanggung Jawab Bank Terhadap Kebocoran Data Nasabah: Ditinjau Dalam Perspektif Hukum Perbankan

Muhammad Wildan[1], Daud Renata Candra Ramadhan[2], Zulfa Rena Wijayanti[3]
[123]Fakultas Hukum Universitas Negeri Semarang
Email: muhwildan1801@students.unnes.ac.id[1], daudrenata@students.unnes.ac.id[2], zulfarenaa@students.unnes.ac.id[3]

Abstract
Kebocoran data nasabah telah menjadi isu penting dalam dunia perbankan modern, dengan dampak signifikan terhadap nasabah dan reputasi bank. Penelitian ini bertujuan untuk menganalisis tanggung jawab hukum bank terhadap kebocoran data nasabah di Indonesia, dengan fokus pada regulasi yang berlaku, seperti Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Metode penelitian yang digunakan adalah yuridis normatif, yang mengkaji kewajiban bank dalam menjaga kerahasiaan dan keamanan data nasabah. Hasil penelitian menunjukkan bahwa bank memiliki kewajiban hukum untuk melindungi data nasabah, termasuk memastikan sistem keamanan yang mampu menghadapi ancaman, seperti serangan siber. Jika bank terbukti lalai, sanksi administratif, pidana, atau ganti rugi dapat dikenakan. Penelitian ini juga mengidentifikasi tantangan implementasi regulasi, seperti kurangnya kepatuhan bank, lemahnya pengawasan, dan rendahnya kesadaran perlindungan data di sektor perbankan.

Article History
Received Okt 27, 2024
Revised Okt 29, 2024
Accepted 09 Nov 2024
Available online 21 Nov. 2024

Keywords :
Kebocoran data, Tanggung jawab hukum, Bank, Perlindungan data pribadi, Hukum perbankan.

Abstract
Data breaches involving bank customers are a critical issue in modern banking, with significant impacts on both customers and the reputation of banks. This study analyzes the legal responsibilities of banks regarding data breaches in Indonesia, focusing on applicable regulations, such as Law No. 10 of 1998 on Banking and Law No. 27 of 2022 on Personal Data Protection (PDP Law). The research employs a normative juridical method to examine banks' obligations to maintain the confidentiality and security of customer data. The findings indicate that banks have a legal duty to protect customer data, including ensuring security systems capable of addressing threats like cyberattacks. Banks found negligent in fulfilling these duties may face administrative sanctions, criminal penalties, or damages. The study also identifies challenges in regulatory implementation, such as non-compliance by banks, weak oversight, and low awareness of data protection in the banking sector.

Keywords :
Data breaches, Legal responsibility, Banks, Personal data protection, Banking law.

https://doi.org/10.5281/zenodo.14201758

PENDAHULUAN

Dalam era digital yang semakin maju seperti saat ini, perlindungan data pribadi nasabah menjadi salah satu aspek yang sangat krusial dalam sektor perbankan. Bank, sebagai lembaga yang berperan penting dalam pengelolaan keuangan masyarakat, memiliki tanggung jawab besar untuk menjaga keamanan data pribadi nasabah. Data ini tidak hanya mencakup informasi dasar seperti nama, alamat, dan nomor telepon, tetapi juga meliputi data finansial yang sangat sensitif, seperti nomor rekening, transaksi keuangan, dan informasi kartu kredit. Dalam konteks ini, data nasabah merupakan bentuk kepercayaan yang diberikan oleh masyarakat kepada bank. Kepercayaan tersebut harus dijaga dengan sebaikbaiknya agar tidak terjadi pelanggaran yang dapat merugikan kedua belah pihak. Namun, kenyataannya, insiden kebocoran data nasabah sering kali terjadi, baik disebabkan oleh serangan siber yang semakin canggih maupun kelalaian internal dari pihak bank sendiri. Serangan siber seperti peretasan data (data breach), phishing, dan malware kini semakin sering menargetkan sistem perbankan, memanfaatkan celah keamanan yang ada untuk mencuri informasi penting. Selain itu, kelalaian internal seperti kesalahan manusia (human error) dalam pengelolaan data, ketidakpatuhan terhadap protokol keamanan, atau penyalahgunaan akses oleh karyawan bank turut menjadi penyebab utama kebocoran data. Dampak dari kebocoran data ini tidak hanya dirasakan

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 392-397

oleh nasabah dalam bentuk kerugian materiil, tetapi juga dapat merusak reputasi bank, mengurangi tingkat kepercayaan masyarakat, serta menimbulkan risiko hukum yang signifikan.

Dalam hukum perbankan di Indonesia, kewajiban bank untuk menjaga kerahasiaan data nasabah telah diatur dengan jelas dalam UndangUndang Nomor 10 Tahun 1998 tentang Perbankan. Undangundang ini secara eksplisit menekankan bahwa bank wajib merahasiakan informasi terkait nasabahnya, kecuali dalam keadaan tertentu yang diatur oleh hukum, seperti permintaan resmi dari lembaga penegak hukum. Di samping itu, UndangUndang Perlindungan Data Pribadi (UU PDP), yang baru disahkan, memberikan kerangka hukum yang lebih spesifik dan komprehensif terkait pengelolaan data pribadi, termasuk kewajiban bank sebagai pengendali data. Regulasi ini mengatur tentang prinsipprinsip pengumpulan, penyimpanan, pemrosesan, dan distribusi data, serta memberikan perlindungan hukum bagi nasabah jika terjadi pelanggaran. Namun demikian, implementasi dari regulasiregulasi tersebut di lapangan masih menghadapi berbagai tantangan. Salah satu tantangan terbesar adalah kurangnya kepatuhan dari pihak bank terhadap standar keamanan yang telah ditetapkan. Beberapa bank mungkin belum sepenuhnya memahami pentingnya investasi dalam teknologi keamanan yang memadai, sehingga rentan terhadap serangan siber. Selain itu, pengawasan oleh otoritas yang berwenang, seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), juga masih perlu ditingkatkan agar mampu memastikan bahwa setiap bank mematuhi regulasi dengan baik. Faktor lain yang juga menjadi kendala adalah kurangnya literasi masyarakat mengenai pentingnya menjaga data pribadi mereka sendiri, sehingga banyak nasabah yang menjadi korban kejahatan siber karena ketidaktahuan.

Melihat kompleksitas permasalahan ini, analisis mendalam mengenai tanggung jawab bank dalam kebocoran data nasabah menjadi sangat penting. Analisis ini bertujuan untuk mengidentifikasi akar permasalahan serta menemukan langkahlangkah perbaikan yang dapat dilakukan oleh bank, regulator, maupun masyarakat secara umum. Beberapa aspek yang perlu dibahas meliputi bagaimana bank dapat meningkatkan sistem keamanan mereka, bagaimana regulasi yang ada dapat diimplementasikan secara efektif, serta bagaimana masyarakat dapat lebih sadar akan pentingnya menjaga data pribadi mereka. Dengan adanya pembahasan yang komprehensif, diharapkan bahwa sektor perbankan di Indonesia dapat menjadi lebih aman, terpercaya, dan mampu melindungi hakhak nasabah secara maksimal. Lebih jauh lagi, dalam konteks global, isu perlindungan data pribadi juga menjadi perhatian utama. Sejumlah negara telah mengadopsi regulasi yang ketat seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang menetapkan standar tinggi dalam perlindungan data pribadi. Hal ini memberikan pelajaran berharga bagi Indonesia untuk terus memperbaiki sistem hukum dan regulasinya agar sejalan dengan perkembangan teknologi dan kebutuhan masyarakat. Oleh karena itu, upaya kolaboratif antara pemerintah, sektor perbankan, dan masyarakat menjadi kunci utama dalam menciptakan ekosistem digital yang aman dan terpercaya.

METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode yuridis normatif, yaitu suatu metode penelitian yang bertujuan untuk mengkaji normanorma hukum yang berlaku dengan pendekatan terhadap peraturan perundangundangan yang relevan. Pendekatan ini dianggap paling tepat karena penelitian difokuskan pada analisis tanggung jawab hukum bank dalam menjaga kerahasiaan data nasabah berdasarkan ketentuan hukum yang berlaku di Indonesia. Dalam hal ini, pendekatan undangundang menjadi kerangka utama untuk memahami bagaimana regulasi yang ada mengatur kewajiban perbankan, serta sejauh mana regulasi tersebut mampu memberikan perlindungan terhadap data pribadi nasabah. Data yang digunakan dalam penelitian ini merupakan data sekunder, yang mencakup sumbersumber hukum tertulis seperti peraturan perundangundangan, literatur hukum, dan berbagai jurnal akademik yang relevan. Peraturan yang menjadi fokus utama penelitian adalah UndangUndang Nomor 10 Tahun 1998 tentang Perbankan, yang mengatur kewajiban bank dalam menjaga kerahasiaan nasabah, serta UndangUndang Perlindungan Data Pribadi (UU PDP), yang memberikan kerangka hukum yang lebih komprehensif terkait pengelolaan dan perlindungan data pribadi. Selain itu, penelusuran terhadap berbagai peraturan pelaksana, seperti peraturan Otoritas Jasa

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 392-397

Keuangan (OJK) dan Bank Indonesia (BI), juga dilakukan untuk memahami bagaimana regulasi diterapkan dalam praktik perbankan.

HASIL DAN PEMBAHASAN

Tanggung Jawab Hukum Bank terhadap Kebocoran Data Nasabah

Dalam sektor perbankan, perlindungan data nasabah merupakan kewajiban yang diatur secara tegas dalam berbagai regulasi. Salah satu dasar hukumnya adalah Pasal 40 UndangUndang Nomor 10 Tahun 1998 tentang Perbankan, yang menyatakan bahwa bank wajib menjaga kerahasiaan data nasabah, kecuali dalam hal tertentu yang diizinkan oleh hukum, seperti untuk kepentingan perpajakan, penyelesaian sengketa perdata, atau permintaan resmi dari aparat penegak hukum. Ketentuan ini menunjukkan bahwa prinsip kerahasiaan nasabah (bank secrecy) adalah landasan utama dalam operasional perbankan, yang harus dihormati demi menjaga kepercayaan masyarakat terhadap sistem perbankan. Namun, dalam kasus kebocoran data, tanggung jawab hukum bank sering kali menjadi perdebatan, terutama ketika insiden tersebut disebabkan oleh kelalaian internal atau serangan siber. Berdasarkan prinsip hukum perdata, tanggung jawab dapat muncul jika kelalaian terbukti menjadi penyebab utama kerugian nasabah. Hal ini sejalan dengan konsep tanggung jawab kontraktual (contractual liability), di mana hubungan hukum antara bank dan nasabah didasarkan pada perjanjian. Dalam perjanjian tersebut, bank berkewajiban untuk menyediakan layanan keuangan dengan tingkat keamanan yang memadai, termasuk melindungi data pribadi nasabah. Apabila kewajiban ini tidak terpenuhi dan nasabah mengalami kerugian, bank dapat dimintai pertanggungjawaban dalam bentuk ganti rugi.

Di sisi lain, UndangUndang Perlindungan Data Pribadi (UU PDP), yang baru disahkan, memberikan kerangka hukum yang lebih spesifik terkait tanggung jawab pengendali data, termasuk bank, dalam mengelola data pribadi. UU PDP mengatur bahwa pengendali data wajib menjaga keamanan data pribadi melalui langkahlangkah teknis dan organisasi yang memadai. Jika terbukti lalai, pengendali data dapat dikenai sanksi administratif berupa denda, pencabutan izin, atau penghentian sebagian aktivitas usaha. Selain itu, UU PDP juga mengatur sanksi pidana untuk pelanggaran serius, seperti penyalahgunaan data atau kebocoran yang disengaja. Dalam konteks ini, bank sebagai pengendali data memiliki tanggung jawab ganda, yaitu tanggung jawab hukum perdata terhadap nasabah yang dirugikan, serta tanggung jawab administratif dan pidana yang dapat diterapkan oleh regulator. Peraturan Otoritas Jasa Keuangan (POJK) Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum juga mengatur aspek keamanan data nasabah sebagai bagian dari manajemen risiko operasional. POJK ini mewajibkan bank untuk memiliki sistem pengendalian internal yang memadai, termasuk kebijakan keamanan informasi, audit internal yang rutin, serta mekanisme mitigasi risiko yang dirancang untuk mencegah kebocoran data. Regulasi ini menekankan bahwa keamanan data bukan hanya tanggung jawab divisi teknologi informasi (IT), tetapi juga merupakan tanggung jawab manajemen secara keseluruhan. Dengan demikian, bank harus memastikan bahwa seluruh lapisan organisasi memahami pentingnya perlindungan data nasabah dan mematuhi prosedur keamanan yang telah ditetapkan.

Dalam praktiknya, penerapan tanggung jawab hukum bank sering kali menghadapi tantangan yang kompleks. Salah satunya adalah sifat insiden kebocoran data yang sering kali sulit untuk dibuktikan secara langsung. Dalam banyak kasus, serangan siber yang menyebabkan kebocoran data dirancang dengan sangat canggih sehingga pelaku sulit dilacak. Selain itu, kelalaian internal seperti kurangnya pelatihan karyawan atau lemahnya pengawasan terhadap vendor pihak ketiga juga menjadi penyebab utama kebocoran data. Dalam situasi seperti ini, bank harus dapat membuktikan bahwa mereka telah melakukan langkahlangkah yang wajar untuk melindungi data nasabah. Jika tidak, mereka dapat dianggap lalai dan bertanggung jawab atas kerugian yang terjadi. Sebagai contoh, dalam beberapa kasus kebocoran data yang pernah terjadi di Indonesia, ditemukan bahwa bank gagal menerapkan protokol keamanan yang memadai, seperti enkripsi data, pembaruan sistem, dan pemantauan aktivitas yang mencurigakan. Hal ini menunjukkan bahwa masih ada celah dalam implementasi regulasi, baik dari sisi kepatuhan bank maupun pengawasan oleh otoritas yang berwenang. Selain itu, faktor lain yang sering kali menjadi penyebab kebocoran data adalah kerja

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 392-397

sama dengan vendor pihak ketiga yang tidak memiliki standar keamanan yang tinggi. Sebagai bagian dari ekosistem perbankan, vendor ini sering kali memiliki akses ke data nasabah, sehingga menjadi titik lemah yang dapat dimanfaatkan oleh pelaku kejahatan siber.

Dalam hal sanksi, penerapan hukuman terhadap bank yang lalai juga masih menjadi tantangan. Di Indonesia, sanksi yang dijatuhkan kepada bank biasanya berupa denda administratif, yang sering kali dianggap tidak cukup memberikan efek jera. Dibandingkan dengan regulasi seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang dapat menjatuhkan denda hingga 4% dari total pendapatan global perusahaan, regulasi di Indonesia masih relatif ringan. Hal ini menunjukkan perlunya penguatan mekanisme penegakan hukum, termasuk peningkatan kapasitas regulator dalam memantau dan menindak pelanggaran. Secara keseluruhan, tanggung jawab hukum bank terhadap kebocoran data nasabah harus dilihat sebagai bagian dari upaya bersama untuk menciptakan ekosistem perbankan yang aman dan terpercaya. Bank harus terus meningkatkan investasi dalam teknologi keamanan, melatih karyawan mereka secara rutin, serta memastikan bahwa vendor pihak ketiga mematuhi standar yang sama. Di sisi lain, regulator perlu meningkatkan pengawasan dan memberikan sanksi yang lebih tegas kepada bank yang melanggar aturan. Dengan langkahlangkah ini, diharapkan kepercayaan masyarakat terhadap sektor perbankan dapat terjaga, sekaligus memberikan perlindungan yang lebih baik bagi nasabah di era digital yang penuh tantangan ini.

Implementasi Regulasi dalam Mencegah Kebocoran Data Nasabah

Implementasi regulasi dalam mencegah kebocoran data nasabah merupakan elemen penting dalam menjaga kepercayaan masyarakat terhadap sektor perbankan di Indonesia. Sebagai salah satu institusi yang memegang data pribadi dalam jumlah besar dan sangat sensitif, bank wajib mematuhi berbagai aturan yang telah ditetapkan oleh pemerintah dan regulator. Salah satu regulasi utama yang menjadi pedoman dalam perlindungan data adalah UndangUndang Perlindungan Data Pribadi (UU PDP). UU ini memberikan kerangka hukum yang jelas bagi pengendali data, termasuk bank, untuk memastikan bahwa data nasabah dikelola dan dilindungi dengan baik melalui penerapan langkahlangkah teknis dan organisasi yang memadai. Langkah langkah teknis yang diwajibkan oleh UU PDP mencakup penggunaan teknologi enkripsi, pembaruan berkala pada sistem keamanan, serta pengendalian akses terhadap data nasabah. Enkripsi, misalnya, merupakan langkah penting untuk memastikan bahwa data yang disimpan atau dikirimkan tidak dapat dibaca oleh pihak yang tidak berwenang. Teknologi ini memberikan lapisan perlindungan tambahan, terutama jika terjadi peretasan. Selain itu, pembaruan sistem keamanan secara berkala diperlukan untuk mengatasi celahcelah yang mungkin dimanfaatkan oleh pelaku kejahatan siber. Teknologi dan taktik yang digunakan oleh peretas terus berkembang, sehingga bank harus mampu mengantisipasi ancaman tersebut dengan melakukan evaluasi dan peningkatan sistem secara berkelanjutan.

Di samping langkah teknis, UU PDP juga menekankan pentingnya langkah organisasi, seperti pelatihan staf secara rutin untuk meningkatkan kesadaran dan pemahaman mereka terhadap pentingnya keamanan data. Karyawan bank sering kali menjadi titik pertama dalam melindungi data nasabah, sehingga pelatihan tentang pengenalan ancaman siber, kebijakan penggunaan perangkat yang aman, dan protokol tanggap darurat saat terjadi insiden sangat diperlukan. Namun, kenyataannya, banyak bank di Indonesia belum sepenuhnya menerapkan standarstandar ini secara konsisten. Hal ini sebagian besar disebabkan oleh minimnya alokasi anggaran untuk keamanan siber, kurangnya pemahaman manajemen akan pentingnya keamanan data, serta budaya kerja yang belum sepenuhnya mendukung penerapan protokol keamanan. Laporan Otoritas Jasa Keuangan (OJK) tahun 2023 mencatat bahwa sekitar 35% dari insiden kebocoran data di sektor perbankan disebabkan oleh kegagalan dalam manajemen risiko siber. Kegagalan ini mencakup berbagai aspek, seperti kurangnya deteksi dini terhadap ancaman, lemahnya pengendalian akses terhadap sistem, hingga ketidaksiapan dalam menanggapi insiden siber. Data ini mencerminkan bahwa meskipun regulasi sudah ada, implementasinya di lapangan masih jauh dari ideal. Salah satu penyebab utamanya adalah kurangnya pengawasan yang ketat dari regulator terhadap kepatuhan bank. Audit reguler terhadap sistem keamanan bank sering kali belum dilakukan secara mendalam, sehingga banyak kelemahan yang tidak teridentifikasi hingga terjadi insiden.

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 392-397

Sebagai pengendali data, bank juga diharapkan memiliki mekanisme mitigasi risiko yang efektif, sebagaimana diatur dalam Peraturan Otoritas Jasa Keuangan (POJK) Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum. POJK ini mewajibkan bank untuk memiliki kebijakan internal yang mencakup identifikasi, penilaian, dan mitigasi risiko terkait keamanan data. Namun, banyak bank yang masih memandang manajemen risiko siber sebagai beban tambahan daripada sebagai investasi strategis. Akibatnya, alokasi sumber daya untuk keamanan sering kali tidak memadai, terutama di bankbank kecil dan menengah yang memiliki keterbatasan anggaran. Selain itu, tantangan dalam implementasi regulasi juga mencakup kerja sama dengan pihak ketiga atau vendor. Banyak bank bekerja sama dengan vendor untuk menyediakan layanan teknologi, seperti cloud storage atau pengelolaan sistem informasi. Namun, tidak semua vendor memiliki standar keamanan yang sesuai dengan regulasi yang berlaku. Hal ini menciptakan titik lemah dalam sistem perlindungan data bank, yang dapat dimanfaatkan oleh pelaku kejahatan siber. Oleh karena itu, bank perlu memastikan bahwa setiap vendor yang mereka gunakan mematuhi standar keamanan yang sama dan tunduk pada audit reguler untuk mengidentifikasi potensi celah keamanan.

Regulasi internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa, dapat menjadi rujukan bagi Indonesia dalam memperbaiki implementasi perlindungan data. GDPR menetapkan standar yang sangat tinggi, termasuk kewajiban pengendali data untuk melaporkan insiden kebocoran data dalam waktu 72 jam setelah kejadian. Selain itu, GDPR juga mendorong pengendali data untuk melakukan penilaian dampak perlindungan data (Data Protection Impact Assessment) secara rutin. Praktikpraktik semacam ini dapat diterapkan di Indonesia untuk memperkuat sistem perlindungan data nasabah di sektor perbankan. Untuk meningkatkan implementasi regulasi, diperlukan upaya yang lebih serius dari berbagai pihak. Bank harus meningkatkan investasi dalam teknologi keamanan dan memastikan bahwa kebijakan internal mereka sejalan dengan regulasi yang berlaku. Regulator seperti OJK dan Bank Indonesia perlu melakukan audit yang lebih ketat dan memberikan sanksi tegas terhadap pelanggaran. Selain itu, diperlukan edukasi kepada masyarakat untuk meningkatkan kesadaran mereka akan pentingnya melindungi data pribadi, sehingga nasabah dapat menjadi mitra aktif dalam menjaga keamanan data.

SIMPULAN

Dalam sektor perbankan, tanggung jawab hukum bank dalam melindungi data nasabah merupakan salah satu elemen penting yang telah diatur secara tegas dalam berbagai regulasi, terutama UndangUndang Nomor 10 Tahun 1998 tentang Perbankan dan UndangUndang Perlindungan Data Pribadi (UU PDP). Berdasarkan ketentuan tersebut, bank wajib menjaga kerahasiaan data nasabah sebagai bentuk penghormatan terhadap hakhak privasi nasabah dan sekaligus sebagai bagian dari kewajiban kontraktual antara bank dan nasabah. Kebocoran data yang terjadi, baik akibat serangan siber maupun kelalaian internal, tidak hanya menimbulkan kerugian material dan immaterial bagi nasabah tetapi juga dapat mengakibatkan sanksi bagi bank. Sanksi tersebut meliputi sanksi administratif berupa denda atau pencabutan izin, hingga sanksi pidana apabila ditemukan pelanggaran yang disengaja atau kelalaian yang signifikan. Hal ini menegaskan bahwa bank memikul tanggung jawab yang besar dalam memastikan perlindungan data pribadi nasabah. Namun demikian, implementasi regulasi yang telah ditetapkan masih menghadapi tantangan besar. Salah satu masalah utamanya adalah lemahnya pengawasan dan kurangnya kepatuhan oleh sejumlah bank dalam menjalankan kebijakan keamanan data sesuai standar yang diatur. Banyak bank yang belum sepenuhnya memprioritaskan keamanan teknologi informasi, baik dalam bentuk investasi pada teknologi canggih maupun dalam pelatihan sumber daya manusia. Kondisi ini diperburuk oleh fakta bahwa serangan siber terhadap sektor perbankan semakin canggih dan terorganisasi, sehingga menuntut bank untuk terus memperbarui sistem keamanan mereka agar tetap relevan dan efektif dalam menghadapi ancaman yang ada.

REFERENSI

Agung, J., & Harun, C. A. (2021). Kebijakan Makroprudensial di Indonesia: Konsep, Kerangka, dan Implementasi-Rajawali Pers. PT. RajaGrafindo Persada.

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 392-397

Atmaja, Y. S., & Paulus, D. H. (2022). Partisipasi Bank Indonesia Dalam Pengaturan Digitalisasi Sistem Pembayaran Indonesia. Masalah-Masalah Hukum, 51(3), 271-286.

Humaidi, A. (2017). Problematika Wewenang Pengawasan Perbankan Dari Bank Indonesia Ke Otoritas Jasa Keuangan. Jurnal Penelitian Hukum Legalitas, 10(2), 53-66

Kusumaningsih, R. (2024). Peran penyidik Otoritas Jasa Keuangan dalam menjaga stabilitas sektor jasa keuangan Indonesia. Jurnal Res Justitia: Jurnal Ilmu Hukum, 4(1), 26-41.

Pikahulan, R. M. (2020). Implementasi fungsi pengaturan serta pengawasan pada Bank Indonesia dan Otoritas Jasa Keuangan (OJK) terhadap perbankan. Jurnal Penegakan Hukum Dan Keadilan, 1(1), 41-51.

Turisno, B. E., & Aminah, Q. E. (2016). Perlindungan Hukum Bagi Konsumen Perbankan dalam Penggunaan Data Pribadi Nasabah (Studi pada PT Bri Kantor Wilayah Semarang). Diponegoro Law Review, 5(3), 19263.

Yustianti, S. (2017). Kewenangan pengaturan dan pengawasan perbankan oleh Bank Indonesia dan Otoritas Jasa Keuangan (OJK). ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan, 1(1), 60-72.