



PELAKSANAAN PELINDUNGAN DATA PRIBADI NASABAH MELALUI LEMBAGA PERBANKAN DI MAKASSAR

Implementation Of Customer Personal Data Protection Through Banking Institutions In Makassar

Syahadat Dahlan^{1*}, Yulia A. Hasan², Almusawir²

¹PT Bank Mega, Tbk Makassar

²Program Studi Ilmu Hukum Program Pascasarjana Universitas Bosowa

*Email: syahadatdahlan@gmail.com

Diterima: 10 Januari 2025/Disetujui: 30 Juni 2025

ABSTRAK

Penelitian bertujuan untuk menganalisis implementasi perlindungan data pribadi nasabah di lingkungan PT Bank Mega, Tbk Makassar dengan menitikberatkan pada tiga aspek utama, yakni proses identifikasi dan verifikasi data, pemrosesan data, serta pengamanan data pribadi nasabah. Dengan menggunakan pendekatan kualitatif dan metode normatif empiris, penelitian ini menggambarkan praktik aktual yang dijalankan oleh lembaga perbankan, serta hambatan yang dihadapi baik dari sisi internal maupun eksternal. Hasil menunjukkan bahwa pelaksanaan perlindungan data dilakukan secara sistematis melalui prosedur operasional yang merujuk pada regulasi perbankan dan standar internal, seperti mekanisme verifikasi berlapis menggunakan alat ABAKA dan formulir persetujuan pemrosesan data. Meskipun terdapat upaya peningkatan perlindungan data, hambatan tetap muncul, antara lain keterbatasan pengetahuan dan integritas karyawan, serta kejahatan siber dari pihak luar yang berupaya membobol sistem keamanan data. Dalam praktiknya, bank telah menetapkan protokol mitigasi seperti pelatihan internal, pembaruan sistem, dan pemeliharaan data berdasarkan klasifikasi risiko nasabah. Penelitian ini menyimpulkan bahwa perlindungan data pribadi memerlukan sinergi antara regulasi yang komprehensif dan pelaksanaan teknis yang berkelanjutan, serta kesiapan sumber daya manusia dalam menghadapi tantangan teknologi digital.

Kata Kunci: Data Pribadi, Pelindungan Nasabah, Keamanan Informasi, Perbankan Digital, Kepatuhan Regulasi

ABSTRACT

This study discusses the implementation of customer personal data protection in PT Bank Mega, Tbk Makassar by emphasizing three main aspects, namely the data identification and verification process, data processing, and securing customer personal data. Using a qualitative approach and empirical normative methods, this study describes the actual practices carried out by banking institutions, as well as the obstacles faced both internally and externally. The results show that the implementation of data protection is carried out systematically through operational procedures that refer to banking regulations and internal standards, such as a layered verification mechanism using the ABAKA tool and a data processing consent form. Despite efforts to improve data protection, obstacles still arise, including limited employee knowledge and integrity, as well as cybercrime from external parties trying to break into the data security system. In practice, the bank has established mitigation protocols such as internal training, system updates, and data maintenance based on customer risk classification. This study concludes that personal data protection requires synergy between comprehensive regulations and ongoing technical implementation, as well as human resource readiness in facing the challenges of digital technology.

Keywords: Personal Data, Customer Protection, Information Security, Digital Banking, Regulatory Compliance



This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

1. PENDAHULUAN

Perlindungan terhadap data pribadi telah menjadi isu hukum global yang penting seiring dengan meningkatnya penggunaan teknologi informasi dalam kehidupan sosial dan ekonomi, termasuk dalam sektor jasa keuangan. Data pribadi merupakan bagian dari hak asasi manusia yang melekat pada setiap individu, sehingga pengelolaannya memerlukan perlakuan hukum yang ketat. Di Indonesia, lahirnya Undang-

Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi tonggak penting dalam menjamin hak warga negara atas informasi pribadinya. Namun, keberadaan regulasi tersebut belum secara spesifik menyentuh sektor perbankan secara mendalam. Mengingat bank merupakan lembaga yang menghimpun dan mengelola informasi sensitif nasabah, perlindungan data pribadi dalam sistem perbankan menjadi krusial untuk menjamin kepercayaan publik. Dalam era digital, data pribadi tidak hanya menjadi objek hukum, tetapi juga

menjadi aset ekonomi yang rentan terhadap penyalahgunaan. Oleh karena itu, isu pelindungan data pribadi menuntut pendekatan hukum yang adaptif terhadap perkembangan teknologi dan dinamika hubungan nasabah dengan lembaga keuangan.

Fenomena kebocoran data pribadi di sektor keuangan menjadi perhatian serius karena dapat mengancam stabilitas keuangan individu maupun integritas lembaga perbankan. Dalam beberapa tahun terakhir, terdapat sejumlah kasus pelanggaran data yang melibatkan institusi besar, termasuk bank, yang memicu kekhawatiran akan lemahnya sistem keamanan digital di Indonesia. Peretasan yang dialami Bank Syariah Indonesia pada 2023 menjadi ilustrasi nyata tentang pentingnya penguatan regulasi dan teknis pelindungan data. Selain itu, kasus penyalahgunaan data oleh oknum internal juga menunjukkan bahwa tantangan tidak hanya datang dari eksternal, tetapi juga dari kelemahan dalam pengawasan dan budaya organisasi itu sendiri. Di Makassar, penggunaan sistem digital dalam transaksi perbankan telah meningkat secara signifikan, namun sistem ini belum sepenuhnya diimbangi dengan mekanisme pelindungan data yang komprehensif. Masyarakat sebagai pengguna layanan memiliki harapan agar data pribadinya dikelola secara aman dan tidak digunakan di luar persetujuan mereka. Dalam konteks ini, pelaksanaan pelindungan data oleh perbankan bukan hanya menjadi tuntutan hukum, tetapi juga kebutuhan operasional dalam menjaga keberlanjutan bisnis.

Kenyataan di lapangan menunjukkan bahwa meskipun telah terdapat sejumlah regulasi dan kebijakan internal bank yang mengatur pelindungan data pribadi, implementasinya masih menghadapi berbagai hambatan. Di PT Bank Mega, Tbk Cabang Makassar, pelaksanaan perlindungan data sudah diatur dalam berbagai dokumen internal, seperti Surat Edaran dan Standar Operasional Prosedur. Namun dalam praktiknya, tidak semua karyawan memiliki pemahaman dan keterampilan yang memadai untuk mengelola data pribadi secara profesional dan bertanggung jawab. Selain itu, ancaman eksternal seperti pemalsuan identitas oleh calon nasabah dan serangan siber dari pihak ketiga menjadi tantangan yang terus meningkat. Di sisi lain, masyarakat juga belum sepenuhnya memahami hak-haknya atas data pribadi, sehingga seringkali tidak menyadari risiko yang dihadapi. Harapan masyarakat akan layanan perbankan yang aman dan terpercaya belum sepenuhnya terwujud apabila perlindungan data tidak menjadi prioritas utama dalam setiap lini pelayanan. Kondisi ini mengindikasikan bahwa upaya perlindungan data harus dilakukan secara menyeluruh dan berkesinambungan.

Masalah utama dalam penelitian ini terletak pada sejauh mana PT Bank Mega, Tbk Makassar melaksanakan perlindungan data pribadi nasabah dalam operasionalnya, serta apa saja kendala yang menghambat pelaksanaan tersebut. Aspek yang dikaji mencakup tahapan identifikasi dan verifikasi, pemrosesan data, dan pengamanan data pribadi. Dalam praktiknya, pelaksanaan perlindungan data pribadi tidak hanya menuntut kesiapan regulasi dan sistem, tetapi juga menuntut kompetensi teknis dan etika dari setiap individu yang terlibat. Fakta bahwa sebagian besar kasus kebocoran data disebabkan oleh kelalaian manusia menandakan perlunya pembenahan dalam aspek sumber daya manusia. Permasalahan ini juga terkait dengan budaya organisasi yang belum menjadikan perlindungan data sebagai prioritas strategis. Penelitian ini menyoroti pentingnya memahami perlindungan data pribadi tidak hanya dari sisi normatif, tetapi juga dari sisi operasional yang konkret.

Berbagai pendekatan telah diupayakan oleh lembaga perbankan untuk menjawab tantangan tersebut. PT Bank Mega, Tbk misalnya, telah mengimplementasikan sistem identifikasi ganda, Customer Information File (CIF), serta prinsip kehati-hatian melalui skema pengawasan berlapis. Instrumen seperti Clear Desk and Clear Screen juga diterapkan untuk mencegah kebocoran data dari lingkungan kerja internal. Di samping itu, klasifikasi risiko nasabah berdasarkan profil bisnis dan aktivitas keuangan telah digunakan untuk menentukan frekuensi pemeliharaan data. Meskipun langkah-langkah tersebut menunjukkan komitmen bank dalam menjaga keamanan data, masih ditemukan celah terutama dalam konsistensi penerapan serta pengawasan terhadap kepatuhan internal. Oleh karena itu, perlu adanya evaluasi terhadap efektivitas sistem yang ada, sekaligus upaya peningkatan kapasitas personalia dan integrasi teknologi pengamanan yang lebih mutakhir.

Terdapat celah penelitian (research gap) yang cukup jelas antara regulasi umum tentang perlindungan data pribadi dan implementasi spesifiknya dalam sektor perbankan. Sebagian besar penelitian terdahulu hanya membahas aspek hukum secara tekstual, tanpa menggali lebih dalam praktik dan tantangan yang dihadapi lembaga keuangan secara empiris. Kajian mengenai perlindungan data di sektor perbankan masih minim, terutama di daerah-daerah seperti Makassar yang memiliki dinamika pelayanan berbeda dengan pusat-pusat keuangan nasional. Penelitian ini hadir untuk mengisi kekosongan tersebut dengan menyajikan data empiris yang diperoleh dari observasi langsung, wawancara mendalam, dan analisis dokumen institusional. Dengan pendekatan ini, studi ini dapat memberikan kontribusi dalam memperkuat dimensi implementasi hukum serta merumuskan strategi perlindungan data yang lebih aplikatif dan responsif terhadap kondisi lokal.

Penelitian bertujuan untuk menganalisis implementasi perlindungan data pribadi nasabah di lingkungan PT Bank Mega, Tbk Makassar dengan menitikberatkan pada tiga aspek utama, yakni proses identifikasi dan verifikasi data, pemrosesan data, serta pengamanan data pribadi nasabah.

2. METODE

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian hukum normatif-empiris. Pendekatan normatif digunakan untuk menelaah peraturan perundang-undangan dan kebijakan internal bank yang mengatur perlindungan data pribadi, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta peraturan dari Bank Indonesia dan Otoritas Jasa Keuangan. Sementara itu, pendekatan empiris digunakan untuk menggambarkan pelaksanaan norma-norma tersebut dalam praktik aktual di lingkungan PT Bank Mega, Tbk Cabang Makassar. Pendekatan ganda ini memungkinkan kajian dilakukan secara menyeluruh, baik dari sisi hukum yang mengatur maupun dari sisi implementasi operasional di lembaga perbankan.

Jenis data dalam penelitian ini terbagi menjadi data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dengan pihak-pihak internal bank, seperti petugas layanan nasabah, manajer kepatuhan, bagian teknologi informasi, serta sejumlah nasabah yang mengalami langsung proses pengelolaan data pribadi. Data sekunder dikumpulkan melalui studi dokumentasi terhadap kebijakan internal bank, formulir persetujuan nasabah, peraturan perundang-undangan, surat edaran, dan dokumen pendukung lain yang berkaitan dengan sistem dan protokol perlindungan data di sektor perbankan.

Pengumpulan data dilakukan dengan menggunakan tiga metode utama, yaitu studi dokumen, untuk menelaah berbagai aturan hukum dan dokumen internal bank yang mengatur perlindungan data pribadi, seperti SK internal, SOP, dan formulir persetujuan. Wawancara mendalam, dilakukan secara semi-terstruktur dengan informan yang dipilih secara purposif, untuk menggali pengalaman dan pemahaman mereka terhadap pelaksanaan perlindungan data pribadi. Observasi partisipatif, dilakukan di area pelayanan nasabah dan sistem pengelolaan data internal, guna memperoleh gambaran faktual tentang implementasi sistem keamanan dan perlindungan data pribadi dalam praktik harian.

Data dianalisis dengan menggunakan analisis deskriptif kualitatif dalam tiga tahap: reduksi data, yaitu proses pemilihan dan penyederhanaan data lapangan yang relevan dengan fokus penelitian, terutama yang menyangkut proses identifikasi, verifikasi, pemrosesan, dan pengamanan data pribadi. Penyajian data, dilakukan dalam bentuk kategorisasi tematik untuk menggambarkan pola-pola dan kecenderungan praktik perlindungan data pribadi di lembaga perbankan. Penarikan kesimpulan, dilakukan secara induktif, dengan mengaitkan hasil temuan empiris dengan kerangka normatif hukum yang berlaku. Proses ini menghasilkan simpulan yang menggambarkan kesenjangan antara regulasi dan praktik serta menawarkan alternatif solusi yang aplikatif.

3. HASIL DAN PEMBAHASAN

3.1. Pelaksanaan Pelindungan Data Pribadi Nasabah pada PT Bank Mega Tbk Di Makassar

Pemerintah telah mengesahkan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, namun pelaksanaannya masih berada pada tahap awal dengan beberapa aspek yang perlu dibenahi. Sebagai perbandingan di negara-negara maju, regulasi perlindungan data pribadi telah mencakup aspek khusus yang berkaitan dengan sektor perbankan, sementara di Indonesia, regulasi yang ada masih bersifat umum dan memerlukan pengaturan lebih rinci untuk sektor perbankan. Selain itu, penerapan hukum yang belum maksimal dan minimnya mekanisme pengawasan menjadi masalah dalam melindungi data nasabah. Fenomena hukum ini menjadi tantangan bagi pemerintah Indonesia dan pelaku usaha (perbankan) untuk tetap mematuhi regulasi yang ada.

Menurut Irwan Kurniawan, Staf legal PT Bank Mega, Tbk Regional Makassar, wawancara tanggal 16 Januari 2025 bahwa: Perkembangan informasi dan teknologi, khususnya konektivitas jaringan, memberikan pengaruh besar dalam kehidupan manusia. Dalam lembaga perbankan memudahkan sistem informasi dan komunikasi, praktis dalam hubungan hukum perbankan dan efisien dalam pelayanan nasabah. Guna melindungi keamanan data nasabah setiap tahap pelayanan di PT Bank Mega, Tbk memiliki standar pelayanan yang dijabarkan dari peraturan Bank Indonesia dan Otoritas Jasa Keuangan (OJK). Oleh karenanya prinsip kehati-hatian dalam perbankan (prudential banking principle) merupakan asas yang mengharuskan bank menjalankan usahanya dengan hati-hati. Prinsip ini bertujuan untuk melindungi data masyarakat dan meminimalkan kerugian bank.

Perkembangan informasi dan teknologi berpengaruh positif terhadap pelayanan jasa perbankan. Namun pada sisi lain, kecanggihan teknologi menjadi ancaman bagi nasabah dan pihak bank apabila penggunaan data pribadi yang terakses

melalui sistem informasi dan teknologi tidak terlindungi secara baik. Hal selaras disampaikan oleh Andi Abdullah Waduud, Pejabat Operasional PT Bank Mega, Tbk (wawancara tgl 4 Januari 2025) bahwa perlindungan data pribadi nasabah pada PT Bank Mega Tbk melalui tahapan operasional sebagai berikut:

a. Identifikasi dan Verifikasi Data Pribadi Nasabah

Implementasi prinsip kehati-hatian dalam memastikan kebenaran informasi atau data pribadi nasabah merupakan hal utama dalam pelayanan PT Bank Mega Tbk. Identifikasi dan verifikasi data pribadi nasabah yang dilakukan oleh Customer Service (CS) pada tahap awal pelayanan, Identifikasi yaitu tindakan mencocokkan data pribadi nasabah dengan dokumen nasabah melalui proses mencari, meneliti dan mencatat data nasabah. Tindakan ini dilakukan untuk melindungi data pribadi nasabah dari pemalsuan identitas. Sedangkan verifikasi yaitu tindakan pengecekan keabsahan dokumen pribadi nasabah dengan menggunakan sistem operasional bank. Verifikasi dapat dilakukan pada tahap awal pelayanan oleh CS dan diverifikasi kembali oleh Pejabat Operasional Bank. Berdasarkan Peraturan Bank Indonesia (BI) No.11/28/PBI/2009 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme bagi Bank Umum (APU dan PPT) secara substansi mewajibkan bank sebelum memberikan pelayanan kepada nasabah terlebih dahulu harus mengenali calon nasabahnya (know your customer). Bank wajib memahami profil, maksud, tujuan nasabah, dan transaksi yang akan dilakukan nasabah melalui tahapan identifikasi dan verifikasi yang dilakukan oleh CS.

Pelayanan nasabah pada semua lembaga bank termasuk di PT Bank Mega, Tbk dilakukan dengan menerapkan prinsip kehati-hatian, selektif dan akurat. Proses awal pelayanan oleh CS wajib dilakukan dengan mengikuti pedoman atau aturan yang telah ditetapkan dalam tata cara penerimaan nasabah. Proses penerimaan dokumen nasabah wajib mengikuti aturan internal bank yang telah dituangkan melalui Standar Operasional Bank (SOP) sebagai implementasi dari ketentuan BI melalui APU dan PPT. Penerapan SOP ini wajib didukung dengan pengetahuan yang memadai dari CS atau staf pelayanan bank baik peraturan umum maupun aturan internal bank. Staf pelayanan bank menerima nasabah dan mengolah data secara terstruktur sesuai urutan yang diarahkan dalam aturan internal bank yang telah ditetapkan pada setiap tahap pelayanan nasabah.

Menurut Andi Abdullah Waduud, Pejabat Operasional PT. PT Bank Mega Tbk (wawancara tanggal 4 Januari 2025), bahwa standar operasional PT Bank Mega, Tbk tentang penerimaan dan pemeliharaan data nasabah dilakukan dengan melalui dua tahap sebagai berikut:

1) Tahap identifikasi data Nasabah

Pada proses identifikasi nasabah atau Customer Due Dilligence (CDD), CS meneliti secara menyeluruh terhadap dokumen nasabah mulai dari keabsahan kartu identitas seperti Kartu Tanda Penduduk (KTP) atau Paspor sampai kesesuaian informasi yang terkadung di dalamnya. KTP merupakan identitas utama seseorang karena kartu tanda penduduk merupakan identitas resmi seorang penduduk sebagai bukti diri yang diterbitkan oleh instansi pemerintah. Paspor merupakan dokumen resmi yang berfungsi sebagai identitas dan kewarganegaraan saat berada di luar negeri. Oleh karena itu kesesuaian nama nasabah

dengan kartu identitas tersebut wajib dipastikan agar tidak terjadi penyalahgunaan identitas.

2) Verifikasi Data Nasabah

Data dan dokumen nasabah yang telah diidentifikasi dan diverifikasi oleh CS pada tahap awal selanjutnya diverifikasi oleh Pejabat Operasional PT Bank Mega, Tbk. Data awal telah dituangkan dalam formulir data nasabah yang sebelumnya telah ditandatangani oleh CS. Pejabat Operasional memeriksa ulang dengan sangat hati-hati dan selektif. Setelah data nasabah diyakini valid, formulir data nasabah dikonfirmasi kembali kepada nasabah perihal kebenaran datanya dan ditandatangani oleh nasabah sebagai bentuk persetujuan datanya akan diproses lebih lanjut. Guna menjamin keaslian dokumen data pribadi nasabah, keabsahan dokumen pribadi diverifikasi melalui alat bantu dan teknologi yang telah disiapkan oleh bank, disebut Alat Baca Kartu (ABAKA). Setelah informasi dan dokumen nasabah valid, nasabah memberikan persetujuan penggunaan data. Hal ini diatur melalui ketentuan Pasal 20 UU PDP bahwa nasabah wajib memberikan persetujuan yang sah secara eksklusif sebelum data pribadinya digunakan. Persetujuan dapat disampaikan secara elektronik maupun non elektronik (secara tertulis). Ketentuan Pasal 20 UU PDP dijabarkan melalui peraturan internal PT Bank Mega, Tbk yaitu Surat Keputusan (SK) Nomor 063/DIRBM/2023 yang mengatur tentang identifikasi nasabah dan persetujuan nasabah dengan menandatangani formulir data nasabah. Tujuan identifikasi dan verifikasi dilakukan yaitu untuk memperoleh kepastian hukum bahwa dokumen yang digunakan nasabah adalah dokumen legal dan yang bersangkutan berhak menggunakan dokumen tersebut sebagai identitas pribadi.

Proses identifikasi nasabah dibenarkan oleh Putri Pertiwi, salah satu nasabah PT Bank Mega Tbk (wawancara tanggal 6 Januari 2025) bahwa: "Identitas saya sebagai nasabah diteliti dengan cermat oleh CS sambil bertanya beberapa hal terkait informasi pribadi dan tujuan ke PT Bank Mega, Tbk. Informasi dan dokumen dicocokkan sebelum menandatangani formulir pembukaan rekening yang saya inginkan". Selanjutnya, Syinthia, Customer Service PT Bank Mega, Tbk, (wawancara 7 Januari 2025) mengutarakan bahwa: "Keaslian kartu identitas diverifikasi dengan cara pengecekan langsung menggunakan alat verifikasi keaslian kartu identitas yang disebut ABAKA. Alat tersebut akan memvalidasi keaslian kartu identitas dengan cara memberikan signal terverifikasi. Jika kartu identitas asli, maka saat yang bersamaan akan menampilkan data serta informasi data pribadi lengkap dari nasabah." Upaya ini sangat membantu untuk mencegah adanya tindakan penyalahgunaan data pribadi orang lain oleh calon nasabah.

3) Pemrosesan Data Pribadi Nasabah

Tahap berikut setelah identifikasi dan verifikasi data pribadi adalah pemrosesan data pribadi nasabah. Berita Acara Identifikasi Data Pribadi Nasabah yang telah disetujui dan ditandatangani oleh nasabah dan CS selanjutnya diverifikasi oleh Pejabat Operasional PT Bank Mega, Tbk untuk memperoleh kepastian bahwa tidak ada kesalahan dalam identifikasi data

nasabah. Sebelum dilakukan penginputan data nasabah, pejabat operasional harus memastikan apakah nasabah tidak terlibat dalam tindak pidana pendanaan terorisme atau tindak pidana pencucian uang (TPPT/TPPU). Dalam tahap ini staf pelayanan memeriksa melalui sistem yang telah disiapkan oleh PT Bank Mega, Tbk sebagaimana ditetapkan melalui Surat Keputusan Nomor SK: 042/DIRBM/20 tanggal 23 Maret 2020 tentang Pedoman Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme/Program APU & PPT. Terhadap nasabah yang data pribadinya telah tervalidasi keabsahannya melalui ABAKA, maka atas persetujuan nasabah data pribadinya akan diproses melalui aplikasi transaksi yang diinginkan oleh nasabah. Namun terhadap nasabah yang terverifikasi data pribadinya terindikasi jaringan teroris atau pencucian uang tidak dapat menggunakan data pribadinya melalui lembaga perbankan atau ditolak menjadi nasabah PT Bank Mega, Tbk bahkan identitas nasabah tersebut dicatat dalam daftar khusus nasabah.

Data pribadi nasabah diproses melalui sistem aplikasi sesuai transaksi yang diminati oleh nasabah seperti aplikasi pinjaman/kredit, aplikasi deposito, aplikasi kartu kredit, melalui Customer Informations File (CIF). Sistem CIF berfungsi untuk mencatat serta mengetahui data-data pribadi, data keuangan, dan data-data yang terkait nasabah lainnya. Data nasabah ini merupakan informasi rahasia bank yang sangat dijunjung tinggi oleh PT Bank Mega, Tbk. Selanjutnya tahapan pemrosesan data nasabah ke dalam sistem bank dilakukan sesuai dengan informasi yang telah disampaikan oleh nasabah yang dituangkan dalam formulir data nasabah yang telah ditandatangani. Pada tahap ini CS tetap melakukan dengan hati-hati untuk menjaga kerahasiaan data nasabah. PT Bank Mega, Tbk bertanggungjawab untuk menjaga kepercayaan nasabah dan memberikan pelayanan yang baik serta mencegah adanya kendala-kendala atau risiko-risiko yang timbul akibat adanya penyalahgunaan data pribadi nasabah. (Irwan Kurniawan, Staf Legal PT Bank Mega, Tbk Regional Makassar, Wawancara 17 Januari 2025).

Sesuai Surat Edaran PT Bank Mega Tbk Nomor: 008/DIRBM-PIMC/25 tanggal 15 Januari 2025 tentang Pemrosesan Data Pribadi Oleh Pihak Ketiga. PT Bank Mega, Tbk dapat menunjuk pihak ketiga sebagai prosesor data pribadi atau pengendali data bersama berdasarkan perjanjian pemrosesan data pribadi (wawancara dengan Irwan Kurniawan, 17 Januari 2025). Perjanjian pemrosesan data pribadi tersebut juga memuat ketentuan terkait transfer data pribadi yang disepakati oleh para pihak. Para pihak yang mengelola transfer data pribadi wajib memastikan instruksi dan persyaratan yang disepakati dilaksanakan dengan tepat, terutama persyaratan keamanan yang terdokumentasi untuk menjaga keamanan data pribadi

Penerapan prinsip kehati-hatian oleh PT Bank Mega, Tbk juga terwujud dalam format perjanjian kredit yang disesuaikan dengan Peraturan OJK No. 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, Dalam perjanjian kredit ditambahkan klausula yang berkaitan dengan persetujuan debitur kepada PT Bank Mega, Tbk dalam rangka pemrosesan data pribadi melalui aplikasi. Dalam hal pembukaan dan/atau penutupan rekening, prinsip kehati-hatian

PT Bank Mega, Tbk dituangkan dalam SK. No. 063/DIRBM/23 tentang Data Nasabah dan Simpanan Dana Pihak Ketiga, yang mengatur tentang tata cara kegiatan operasional yang berkaitan dengan data nasabah dan simpanan dana pihak ketiga di PT Bank Mega, Tbk serta menjadi acuan satuan kerja dalam menjalankan proses transaksi dan internal audit.

b. Pengamanan Data Pribadi Nasabah

Untuk mengatasi penyalahgunaan data nasabah PT Bank Mega, Tbk menerapkan aturan yang disebut Clear Desk and Clear Screen dengan mengeluarkan Surat Edaran PT Bank Mega, Tbk No.284 Tahun 2024 tentang Clear Desk dan Clear Screen. Tujuan Surat Edaran ini agar semua karyawan termasuk unsur pimpinan bertindak hati-hati menjaga data pribadi nasabah sekaligus juga rahasia PT Bank Mega Tbk. Pihak-pihak yang memiliki kewajiban untuk menjaga kerahasiaan informasi keuangan nasabah dan simpanan diatur dalam Pasal 47 ayat (2) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yaitu "Anggota Dewan Komisaris, Direksi, pegawai bank, atau pihak terafiliasi lainnya." Menurut Pasal 47 ayat (2), yang dimaksud dengan pegawai bank adalah semua pejabat dan karyawan yang bekerja di bank. Melalui Surat Edaran PT Bank Mega, Tbk No.284 Tahun 2024 mewajibkan semua karyawan sebelum meninggalkan meja, ruangan kerja, tempat menggandakan dokumen harus merapikan dokumen, memproteksi dokumen, data/informasi confidential/strictly confidential bank dengan tujuan untuk mengurangi potensi risiko pelanggaran, penyalahgunaan, dan pencurian data/ informasi nasabah dari internal bank. Surat Edaran ini sebagai upaya preventif tindakan penyalahgunaan data pribadi nasabah dari internal bank.

Tahap pengamanan data pribadi nasabah meliputi kegiatan pemeliharaan data nasabah karena tindakan pemeliharaan data berorientasi data yang update. Data Nasabah baik hard copy maupun soft copy yang telah terinput dalam sistem aplikasi CIF PT Bank Mega Tbk dilakukan pemeliharaan secara berkala untuk menjaga kesesuaian data dengan kondisi terkini (up to date) dari data nasabah. Proses pemeliharaan data tersebut dilakukan sesuai tingkat risiko dari nasabah. Klasifikasi nasabah berdasarkan tingkat risiko yaitu nasabah berisiko tinggi, nasabah berisiko menengah dan nasabah berisiko rendah. Nasabah berisiko tinggi adalah nasabah yang mempunyai bisnis yang dikategorikan tinggi seperti penjual emas, pemilik money changer, anggota TNI, Polri, dll. Nasabah berisiko sedang adalah nasabah yang memiliki beberapa faktor yang perlu diwaspadai terkait peluang pencucian uang atau pendanaan terorisme sedang nasabah berisiko rendah adalah nasabah yang tidak berpotensi melakukan tindak pidana terorisme atau pencucian. Bagi nasabah kategori high risk (risiko tinggi) dilakukan pemeliharaan data setiap 1 (satu) tahun sekali. Bagi nasabah berisiko sedang dilakukan pemeliharaan data satu kali dalam dua tahun sedangkan nasabah yang memiliki kategori berisiko rendah dilakukan pemeliharaan data satu kali dalam lima tahun. Perubahan data nasabah dilakukan dengan tujuan untuk kekinian data atau koreksi kesalahan data.

Menurut Irwan Kurniawan, Staf Legal Regional Makassar, (Wawancara 17 Januari 2025) bahwa, untuk mencegah hambatan pelaksanaan perlindungan data pribadi nasabah, PT Bank Mega, Tbk menerapkan kontrol pengawasan yang ketat pada saat penerimaan data nasabah yang dituangkan dalam aturan internal Surat Keputusan No. 063/DIRBM/23

bahwa: CS yang menangani proses operasional pendaftaran nasabah baru, wajib melakukan pemeriksaan terhadap kelengkapan, keabsahan, kebenaran dokumen nasabah, Supervisor/Pejabat Operasional sesuai jenjang kewenangannya wajib melakukan pengawasan masing-masing unit kerja guna memastikan seluruh proses dilakukan dengan benar sesuai ketentuan dan CS berkewajiban melakukan review arsip data nasabah secara periodik

3.2. Hambatan Pelaksanaan Pelindungan Data Pribadi Nasabah pada PT Bank Mega Tbk Makassar

Perkembangan teknologi saat ini membawa berbagai keuntungan, termasuk dalam dunia perbankan yang menawarkan layanan lebih cepat dan praktis. Dengan adanya layanan digital, nasabah tidak perlu lagi datang langsung ke bank dan berinteraksi secara tatap muka dengan karyawan bank untuk melakukan transaksi. Di sisi lain ancaman kejahatan siber tetap menjadi risiko yang bisa dialami oleh nasabah/bank. Walaupun bank menerapkan protokol keamanan yang ketat, potensi tindak kejahatan tetap ada dan hambatan dalam pelaksanaan pelindungan data pribadi nasabah dapat terjadi.

a. Hambatan Internal

1) Pengetahuan dan Keterampilan

Berkaitan dengan pelindungan data nasabah sangat didukung oleh tingkat pengetahuan atau pemahaman karyawan dalam hal ini CS dalam menjalankan tugas dan tanggungjawabnya sesuai aturan internal PT Bank Mega, Tbk. Setiap aktifitas penerimaan nasabah oleh CS telah diatur secara detail yang tidak bisa dilanggar. Kelalaian CS yang melakukan pelayanan awal identifikasi data dapat mengakibatkan masalah besar baik bagi nasabah maupun bank itu sendiri.

Customer service dan karyawan Pt.Bank Mega Tbk lainnya yang secara sengaja atau tidak sengaja membocorkan informasi identitas pribadi nasabah/pelanggan kepada pihak lain baik di lingkungan kerja sendiri atau di luar lingkungan kerja PT Bank Mega, Tbk yang mengakibatkan terungkapnya nomor telepon pelanggan, nama lengkap, saldo bank, dan data pribadi sensitif lainnya. akan dikenakan sanksi sesuai klasifikasi tindakan atau pelanggaran seperti sanksi pidana, perdata maupun sanksi administrasi.

Hambatan pelaksanaan pelindungan data pribadi nasabah yaitu adanya kecerobohan CS atau karyawan PT Bank Mega Tbk lainnya dalam proses penggandaan dokumen sebagai syarat tambahan penyimpanan data juga dapat terjadi kapan saja. Tindakan ini dapat menyebabkan kebocoran data nasabah, yang seharusnya menjadi informasi rahasia. Akibatnya, nasabah bisa mengalami kerugian besar karena penyalahgunaan informasi pribadi atau bahkan penipuan. CS atau karyawan bank lainnya yang meninggalkan dokumen sensitif atau data nasabah di meja kerja yang mengakibatkan orang lain dapat mengakses data tersebut. Kejadian demikian, CS atau karyawan lainnya bukan hanya melanggar protokol pelindungan data perusahaan, tapi juga berpotensi membahayakan informasi penting yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Kurangnya kesadaran akan pentingnya menjaga kerahasiaan data perusahaan adalah hambatan utama pelindungan data pribadi nasabah dan akibatnya dapat merusak reputasi serta kepercayaan nasabah.

Pelanggaran seperti ini juga menimbulkan kekhawatiran serius tentang protokol keamanan data nasabah dan berpotensi menyebabkan kerugian finansial bagi nasabah yang terkena dampak. Investigasi menyeluruh diperlukan untuk menentukan

penyebab utama kebocoran tersebut dan menerapkan langkah-langkah yang tepat untuk menyelesaikan masalah dan mencegah kejadian serupa di masa mendatang (tindakan represif).

2) Integritas Karyawan Bank

Pelayanan nasabah di PT Bank Mega, Tbk membutuhkan kemampuan dan kecerdasan dari staf CS dan karyawan lainnya. Tanpa memiliki kecerdasan atau skill yang memadai akan sulit mencapai tujuan pelindungan data pribadi nasabah. Selain membutuhkan skill yang memadai dari seorang CS dan karyawan lainnya hal yang tidak kalah pentingnya adalah kedisiplinan dan tanggung jawab (integritas) dari karyawan bank. Tujuan pelindungan data pribadi nasabah akan tercapai jika CS dan karyawan bank lainnya menjalankan semua urutan pelayanan nasabah secara disiplin sesuai aturan internal bank. Pelindungan data pribadi nasabah harus didukung oleh integritas dari seluruh karyawan PT Bank Mega, Tbk. Data pribadi nasabah akan sangat terexpose risiko penyalahgunaan data pribadi jika karyawan yang memberikan pelayanan tidak jujur. Lemahnya integritas karyawan bank merupakan hambatan internal dalam penerapan pelindungan data pribadi nasabah,

Tindakan pencegahan yang telah dilakukan oleh PT Bank Mega, Tbk sehubungan dengan hambatan-hambatan tersebut adalah pada saat penerimaan karyawan baru akan dilakukan pembekalan In House Training dan Job Training. Hal tersebut dilakukan untuk menambah pengetahuan perbankan dan keterampilan karyawan baru tersebut dalam melayani nasabah. Selain training job, pengecekan berkala dokumen data nasabah sesuai klasifikasinya termasuk tindakan pencegahan terjadinya penyalahgunaan data pribadi nasabah. Data nasabah diperiksa secara keseluruhan melalui proses pemeriksaan yang telah ditetapkan (tindakan preventif PT Bank Mega, Tbk).

Tindakan tersebut untuk mengurangi data pribadi nasabah yang kadaluarsa, perubahan profil nasabah, perubahan alamat, perubahan nomor telepon dan perubahan lainnya. Data nasabah yang berubah segera dihubungi untuk datang ke kantor PT Bank Mega, Tbk melakukan perubahan data dengan mengisi formulir perubahan data. Nasabah yang tidak bisa dihubungi melalui telepon akan dikunjungi ke alamat sesuai yang tertera di sistem bank.

Hambatan lain yang dihadapi oleh karyawan bank bagian pemeliharaan data nasabah yaitu nasabah yang tidak mau lagi datang ke kantor PT Bank Mega, Tbk karena tabungan bank sudah tidak ada lagi sehingga nasabah menganggap tidak perlu lagi datang ke kantor PT Bank Mega, Tbk. Dalam kondisi seperti ini petugas membuat berita acara kunjungan nasabah yang berisikan informasi nasabah tidak mau datang lagi ke PT Bank Mega, Tbk. Selanjutnya CS melaporkan kondisi tersebut ke pejabat operasional untuk diambil tindakan atas data pribadi nasabah. Selanjutnya Data pribadi nasabah yang telah expire atau kadaluarsa dan nasabah tidak mau datang lagi ke PT Bank Mega, Tbk maka, data pribadi nasabah dipisahkan penyimpanannya untuk dilakukan monitoring lebih lanjut.

Menghadapi berbagai hambatan pelindungan data pribadi nasabah dapat diatasi dengan meningkatkan pemahaman karyawan tentang keamanan siber, bank dapat mengurangi risiko kebocoran data akibat kesalahan manusia serta memastikan kesiapan mereka dalam menghadapi ancaman siber. Pelatihan yang berkelanjutan dan rutin juga diperlukan agar karyawan selalu mengikuti perkembangan terbaru dalam teknologi dan ancaman siber, sehingga mereka dapat lebih efektif dalam menjaga keamanan data pribadi nasabah. Memberikan pelatihan secara berkala tentang keamanan siber

kepada karyawan adalah langkah penting untuk meningkatkan kesadaran dan pemahaman mereka tentang pelindungan data pribadi. Materi pelatihan dapat mencakup cara mengenali serta menghindari ancaman siber, seperti phishing, malware, dan serangan rekayasa sosial. Selain itu, pelatihan juga harus mencakup prosedur penanganan kebocoran data, termasuk langkah mitigasi, pelaporan insiden, dan proses pemulihan data.

Infra struktur yang disediakan oleh perbankan memiliki peran penting, terutama dalam memberikan perlindungan kepada nasabah. Namun, dalam penerapannya, aspek keamanan data/dokumen harus menjadi perhatian utama. Jika keamanan tidak dijaga dengan baik, masalah di kemudian hari dapat muncul, yang berpotensi menimbulkan keluhan dari nasabah. Berdasarkan POJK Nomor 18/POJK.07/2018 tentang Layanan Pengaduan Konsumen di Sektor Jasa Keuangan pada Pasal 1, bahwa keluhan atau komplain dari nasabah terhadap layanan yang tidak sesuai dengan harapan, terutama jika mengakibatkan kerugian finansial, disebut sebagai pengaduan. Pengaduan ini bisa disampaikan secara lisan maupun tertulis kepada pihak penyedia layanan, termasuk dalam sistem perbankan berbasis internet banking.

b. Hambatan Eksternal

1) Pemalsuan Identitas Oleh Calon Nasabah

Pelindungan data pribadi nasabah juga tidak lepas dari hambatan pihak eksternal Bank. Gangguan dan hambatan dari pihak eksternal bisa terjadi dari tindakan langsung atau tidak langsung. Calon nasabah yang datang membawa identitas orang lain/palsu dan berusaha menggunakannya atas diri sendiri sangat berisiko untuk pelindungan data pribadi. Jika hal tersebut lolos dari proses identifikasi dokumen dan verifikasi oleh CS atau karyawan lainnya akan menjadi hal yang sangat berbahaya saat data dan dokumen digunakan untuk melanggar hukum, Membuka rekening dengan memakai dokumen orang lain dengan tujuan penipuan, akan membahayakan nama baik pemilik dokumen yang sebenarnya. Hal ini merupakan hambatan nyata secara eksternal dalam rangka pelindungan data pribadi.

2) Pembobolan Data Pribadi Nasabah Secara Eksternal

Pembobolan data pribadi oleh pihak eksternal dapat terjadi juga melalui sistem bank atau aplikasi lainnya. Dalam hal ini pelaku melakukan dengan cara phising. Phising adalah kejahatan berbentuk komunikasi palsu yang tampaknya berasal dari phising sumber dipercaya. Tapi sebenarnya dapat membahayakan semua jenis sumber data. Phising bisa mengambil akses ke akun online dan data pribadi seperti Nomor Induk Kependudukan (NIK), nomor kartu kredit, ATM, atau data penting lainnya.

Terkadang korban phising tidak sadar bahwa ia adalah sasaran kejahatan. Korban phising akan memberikan data sensitif seperti informasi identitas pribadi, detail kartu kredit dan perbankan, dan kata sandi. Informasi tersebut kemudian digunakan untuk mengakses akun penting dan dapat mengakibatkan pencurian identitas dan kerugian finansial. Phising dapat dihindari dengan cara mengubah kata sandi secara berkala, menghindari memberikan informasi pribadi kepada pihak yang tidak dikenal, memverifikasi keamanan situs.

Pelaku kejahatan pencurian data pribadi dengan menelpon korbannya mengatasnamakan bank selanjutnya dengan mengiming-iming hadiah sehingga korban terpengaruh bujuk rayu dan dengan suka rela nasabah memberikan data pribadi berupa PIN Transaksi, OTP, atau PIN ATM. Selanjutnya pelaku mengarahkan korban melakukan transaksi lalu

kemudian sejumlah dana dari korban akan hilang tanpa jejak. Hal tersebut dapat dihindari dengan cara tidak memberikan data apapun yang diminta dan selanjutnya segera mendatangi kantor bank terdekat untuk meminta konfirmasi dari kejadian seperti itu. Minta arahan dari customer service apa yang sebaiknya dilakukan untuk mengamankan data pribadi korban. Seorang nasabah datang ke bank dengan tujuan mengganti data yang telah tercatat di bank namun data yang akan diganti milik orang lain. Hal tersebut juga merupakan tantangan dari eksternal bank untuk menjaga data pribadi milik nasabah yang sebenarnya.

Langkah langkah pengamanan untuk mencegah pencurian data dengan model seperti itu PT Bank Mega, Tbk telah melakukan pengamanan yang ketat untuk menghindari pengambilalihan data. Secara selektif nasabah akan diidentifikasi dan diverifikasi sehubungan permintaan perubahan data pribadi sehingga usaha pemalsuan atau usaha pengambilalihan data dapat di cegah dan dihindari. Risiko yang akan timbul dikemudian hari jika pelaku berhasil merubah data atau lolos dari identifikasi dan verifikasi oleh petugas bank maka pelaku dengan leluasa menguasai data pribadi korban yang ada di bank dan dengan leluasa melakukan transaksi atau melakukan penipuan di rekening milik korban

Apapun risiko yang mungkin terjadi dalam operasional bank akan menjadi tanggung jawan penyelenggara jasa perbankan. Jika seorang nasabah mengalami kerugian, pihak bank bertanggung jawab dan bisa dihadapkan pada gugatan dari nasabah tersebut. Bank wajib memberikan ganti rugi kepada nasabah yang menderita kerugian. Ketentuan mengenai tanggung jawab bank dalam menjaga dana nasabah dapat ditemukan dalam peraturan-peraturan yang ditetapkan oleh Bank Indonesia, termasuk dalam peraturan yang lebih spesifik. Peraturan Bank Indonesia Nomor 16/1/PBI/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran dalam Pasal 10 menyatakan bahwa penyelenggara wajib bertanggung jawab kepada konsumen atas kerugian yang timbul akibat kesalahan pengurus dan pegawai penyelenggara. Menurut Ni Putu Denisy, hal ini menunjukkan bahwa penyelenggara memiliki kewajiban sepenuhnya atas berbagai kendala atau permasalahan yang muncul akibat layanan yang mereka sediakan, sehingga hak-hak konsumen tetap terjamin.

4. KESIMPULAN DAN SARAN

Hasil penelitian dapat disimpulkan bahwa pelaksanaan perlindungan data pribadi nasabah oleh PT Bank Mega, Tbk Cabang Makassar telah dilakukan melalui serangkaian prosedur internal yang cukup sistematis, mencakup proses identifikasi, pemrosesan, serta pengamanan data nasabah. Mekanisme yang diterapkan mencerminkan adanya upaya kelembagaan dalam mematuhi prinsip-prinsip kehati-hatian dan menjaga kerahasiaan informasi yang bersifat sensitif. Sistem verifikasi ganda, pelatihan personel, serta penggunaan perangkat pengamanan digital menunjukkan adanya komitmen institusional dalam menjaga kepercayaan publik. Namun demikian, sejumlah kendala masih ditemukan, terutama pada aspek sumber daya manusia, efektivitas pengawasan, serta kesiapan menghadapi potensi serangan dari luar. Tantangan ini memperlihatkan bahwa perlindungan data pribadi memerlukan kesatuan antara aspek hukum, teknis, dan budaya organisasi yang kuat. Dalam konteks ini, perlindungan data pribadi tidak hanya menjadi kewajiban formal, tetapi juga

menjadi fondasi kepercayaan dalam relasi antara nasabah dan lembaga perbankan.

Pelaksanaan perlindungan data belum sepenuhnya optimal karena masih terdapat celah yang memungkinkan terjadinya kebocoran informasi, baik akibat kelalaian petugas maupun serangan eksternal yang tidak terdeteksi. Ketidaksadaran sebagian karyawan terhadap pentingnya menjaga privasi nasabah juga menjadi faktor yang melemahkan sistem pengamanan. Selain itu, belum meratanya sosialisasi kepada nasabah mengenai hak atas data pribadi menyebabkan rendahnya partisipasi publik dalam pengawasan. Upaya perlindungan belum dapat dikatakan efektif apabila belum dibarengi dengan peningkatan kesadaran kolektif di tingkat operasional. Perlindungan data pribadi akan lebih kuat jika dibangun sebagai bagian integral dari kultur pelayanan dan sistem pengelolaan risiko yang konsisten. Oleh sebab itu, peningkatan efektivitas perlindungan data perlu diarahkan pada penguatan regulasi internal, optimalisasi teknologi informasi, serta transformasi sikap dan perilaku seluruh elemen organisasi.

5. DAFTAR PUSTAKA

- Angraini, N., Makkawaru, Z., & Almusawir. (2024). Perlindungan Hukum Data Pribadi dalam Perspektif Hak Asasi Manusia. *Indonesian Journal of Legality of Law*, 7(1), 46–51. <https://doi.org/10.35965/ijlf.v7i1.5267>
- Bhoki, A., Aloysius, S., & Bire, C. M. (2024). Perlindungan Hukum Terhadap Kebocoran Data Nasabah Ditinjau dari Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan. *Petitum Law Journal*, 2(1), 245–256.
- Denisy, N. P., Budiarta, I. N. P., & Putra, I. M. A. M. (2024). Perlindungan Hukum Terhadap Data Pribadi Nasabah Oleh Bank Dalam Transaksi Melalui Internet Banking. *Jurnal Preferensi Hukum*, 5(2), 246–252. <https://doi.org/10.22225/jph.5.2.8088.246-252>
- European Union Agency for Fundamental Rights and Council of Europe. 2014. *Handbook on European Data Protection Law*. Belgium. hal. 36
- Fadhilina, A., Resentia, R., Rukhsal, S. F., Hadiwibowo, H., & Azzahra, A. S. (2024). Perlindungan Data Pribadi Nasabah dalam Transaksi Central Bank Digital Currency (CBDC) dalam Rupiah Digital. *Unes Law Review*, 7(1), 307–317.
- Hanafitty, & Rahayu, S. (2021). Analisis Perlindungan Kerahasiaan Data Pribadi pada Nasabah Pengguna Produk Layanan Mobile Banking Bank Milik Pemerintah Daerah Aceh. *Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan*, 5(2), 328–337.
- Islami, M. J. (2017). Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index. *Jurnal Masyarakat Telematika Dan Informasi*, 8(2), 137–144.
- Katiandagho, V., Diana Darmayanti Putong, & Isye Junita Melo. (2023). Undang – Undang Perlindungan Data Pribadi Memperkuat Undang – Undang Perbankan Dalam Menjaga Rahasia Data Nasabah Dan Untuk Melindungi Data Pribadi Masyarakat Indonesia. *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat*, 9(1), 106–114.

- Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *Jurnal Al-Wasath*, 2(1), 19–32. <https://doi.org/10.47776/alwasath.v2i1.127>
- Lestari, T., Muhti, S., & Yuliansyah, R. (2024). Pertanggungjawaban Perbankan Dalam Melindungi Data Pribadi Nasabah Akibat Peretasan Studi Kasus Bank Syariah Indonesia. *Doktrin: Jurnal Dunia Ilmu Hukum Dan Politik*, 2(3), 48–59.
- Maisah, Sari, S. P., Sudiarni, & Ompusunggu, H. P. (2023). Analisis Hukum Terhadap Perlindungan Data Pribadi Nasabah dalam Layanan Perbankan Digital di Indonesia. *Aufklarung: Jurnal Pendidikan*, 3(3), 285–290.
- Nababan, V., Wulandari, A., & Karlina, L. (2024). Perlindungan Data pribadi nasabah di industri perbankan. *Jurnal Ilmu Hukum*, 1(4), 234–240.
- Nasution, R. A., Ginting, B., Siregar, M., & Azwar, T. K. D. (2024). Perlindungan Hukum Terhadap Data Pribadi Nasabah Layanan Perbankan Setelah Berlakunya Peraturan Otoritas Jasa Keuangan (POJK) Nomor 6/Pojk.O7/2022. *Journal of Education, Humaniora and Social Sciences (JEHSS)*, 7(1), 71–78. <https://doi.org/10.34007/jehss.v7i1.2292>
- Rahmadani, A. E., Pangestu, Y., & Halizhah, N. (2024). Perlindungan Data Pribadi Dalam Era Digital: Tantangan dan Solusi dalam Sistem Perbankan. *Media Hukum Indonesia (MHI)*, 2(4), 180–186.
- Rizky P. Karo Karo dan Teguh Prasetyo. 2020. *Pengaturan Perlindungan Data Pribadi di Indonesia; Perspektif Teori Keadilan Bermartabat*, Penerbit Nusa Media, Bandung. hal. 50
- Tanjung, R. D., & Nurhilmiah. (2024). Aspek Pelindungan Hukum Atas Data Pribadi Nasabah pada Penyelenggaraan Layanan Mobile Banking pada PT. Bank Rakyat Indonesia Cabang Stabat. *Jurnal Ilmu Hukum, Humaniora Dan Politik*, 4(5), 1474–1482.
- Satjpto Rahardjo. 2023. *Permasalahan Hukum di Indonesia*. Alumni. Bandung. hal 121.
- Tasman, S. R., Makkawaru, Z., & Hasan, Y. A. (2021). Analisis Penyelesaian Kredit Bermasalah Pada Bank Bni 46 Cabang Polewali Mandar. *Indonesian Journal of Legality of Law*, 3(2), 63–67. <https://doi.org/10.35965/ijlf.v3i2.640>.