Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer
Volume 6, Nomor 1, Maret 2026
e-ISSN: 2827-7953; p-ISSN: 2827-8135, Hal. 65-73
DOI: https://doi.org/10.55606/juisik.v6i1.2012
Tersedia: https://journal.sinov.id/index.php/juisik

Analisis Pelanggaran Privasi Data Nasabah Akibat Serangan Siber Pada Aplikasi *Mobile Banking*

(Studi Kasus: Bank Syariah Indonesia 2023)

Dimas Wijanarko[1*], Achmad Dhafikrie Solahuddin[2], Haykal Alvito Wibowo[3], Habillah Hasbi Maulana[4], Gilang Ramadhan[5]
[1-5]Prodi Sistem Informasi, Fakultas Teknik & Informatika, Universitas Bina Sarana Informatika, Indonesia
**Penulis Korespondensi: dmswijanarko@gmail.com*

Abstract. *This study aims to evaluate a customer data privacy breach resulting from a cyberattack on Bank Syariah Indonesia's (BSI) mobile banking application in 2023. A ransomware attack carried out by the LockBit 3.0 group resulted in a 1.5 terabyte data leak and disrupted BSI's digital service system across the country. The research approach used was a qualitative descriptive case study to understand the causal factors, the types of breaches that occurred, and the mitigation measures taken by the bank. The results indicate that the privacy breach occurred due to weaknesses in the internal security system, delays in system updates, a lack of end-to-end encryption implementation, and low security awareness among both users and employees. Mitigation measures included security audits, collaboration with the National Cyber and Crypto Agency (BSSN), firewall strengthening, and digital security education for customers. These findings underscore the importance of collaboration between technology, regulation, and digital literacy in strengthening personal data protection in the banking sector. Consistent implementation of the Personal Data Protection Law (Law No. 27 of 2022) is key to building a safe, reliable, and ethical mobile banking ecosystem in Indonesia.*

Keywords: *Bank Syariah Indonesia; Cyber Attacks; Data Privacy; Mobile Banking; Personal Data Protection*.

Abstrak. Penelitian ini memiliki tujuan untuk mengevaluasi pelanggaran privasi data pelanggan yang terjadi akibat penyerangan siber pada aplikasi perbankan mobile Bank Syariah Indonesia (BSI) pada tahun 2023. Serangan jenis ransomware yang dilakukan oleh kelompok LockBit 3.0 menghasilkan kebocoran data sebesar 1,5 terabita dan mengganggu sistem layanan digital BSI secara menyeluruh di seluruh negeri. Pendekatan penelitian yang diterapkan adalah deskriptif kualitatif dengan metode studi kasus, untuk memahami faktor penyebab, jenis pelanggaran yang terjadi, dan langkah-langkah mitigasi yang dilakukan oleh pihak bank. Hasil dari penelitian ini menunjukkan bahwa pelanggaran privasi terjadi akibat kelemahan dalam sistem keamanan internal, keterlambatan dalam pembaruan sistem, kurangnya penerapan enkripsi dari ujung ke ujung, serta rendahnya kesadaran terhadap masalah keamanan baik dari pengguna maupun karyawan. Tindakan mitigasi yang dilakukan mencakup audit keamanan, kolaborasi dengan Badan Siber dan Sandi Negara (BSSN), penguatan firewall, serta pendidikan tentang keamanan digital untuk para nasabah. Penemuan ini menegaskan pentingnya kolaborasi antara teknologi, regulasi, dan literasi digital dalam memperkuat perlindungan data pribadi di dunia perbankan. Penerapan yang konsisten dari Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) menjadi kunci untuk membangun ekosistem perbankan mobile yang aman, dapat diandalkan, dan beretika di Indonesia.

Kata kunci: Bank Syariah Indonesia; Mobile Banking; Perlindungan Data Pribadi; Privasi Data; Serangan Siber.

1. LATAR BELAKANG

Mobile banking merupakan inovasi layanan perbankan berbasis teknologi yang memungkinkan nasabah melakukan transaksi keuangan melalui perangkat seluler secara cepat, efisien, dan aman. Menurut Rahmahdhani et al. (2022), mobile banking hadir sebagai bentuk transformasi digital yang mendukung kemudahan nasabah dalam mengakses layanan keuangan di era modern, tanpa harus datang ke kantor cabang. Namun, kemajuan teknologi ini juga membawa tantangan baru, terutama terkait dengan keamanan data dan privasi pengguna.

Dalam konteks digitalisasi perbankan, privasi data nasabah menjadi aspek krusial yang harus dilindungi oleh lembaga keuangan. Data nasabah mencakup informasi pribadi seperti

Naskah Masuk: 05 Desember 2025; Revisi: 31 Desember 2025; Diterima: 18 Januari 2026;
Tersedia: 20 Januari 2026

nama, alamat, nomor rekening, hingga riwayat transaksi yang sifatnya rahasia. Menurut Hutagaol et al. (2023), lemahnya sistem keamanan dan rendahnya kesadaran pengguna terhadap ancaman siber dapat meningkatkan risiko kebocoran data dalam layanan digital, termasuk mobile banking.

Beberapa tahun terakhir, Indonesia menghadapi peningkatan jumlah serangan siber terhadap lembaga keuangan. Salah satu kasus terbesar terjadi pada Bank Syariah Indonesia (BSI) pada tahun 2023. Berdasarkan laporan Kompas.id (2023), data pribadi nasabah dan pegawai BSI diduga bocor setelah serangan ransomware yang menyebabkan gangguan layanan mobile banking selama beberapa hari. Insiden tersebut memunculkan kekhawatiran publik terhadap keamanan data pribadi dan efektivitas sistem perlindungan privasi yang diterapkan oleh bank.

Meskipun pemerintah telah memberlakukan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), implementasinya dalam sektor perbankan masih menghadapi berbagai kendala. Menurut Nasution (2023), masih banyak lembaga keuangan yang belum sepenuhnya menerapkan prinsip keamanan data sesuai regulasi, terutama dalam konteks kesiapan infrastruktur digital dan pelatihan sumber daya manusia.

Berdasarkan kondisi tersebut, perlu dilakukan penelitian yang menganalisis lebih dalam mengenai pelanggaran privasi data nasabah akibat serangan siber pada aplikasi mobile banking, khususnya pada kasus Bank Syariah Indonesia tahun 2023. Penelitian ini diharapkan dapat memberikan pemahaman mengenai bentuk pelanggaran privasi yang terjadi, faktor penyebabnya, serta upaya mitigasi yang dapat dilakukan untuk memperkuat perlindungan data nasabah di masa mendatang. Rumusan Masalah dari penelitian ini adalah Bagaimana bentuk dan dampak pelanggaran privasi data nasabah akibat serangan siber pada aplikasi mobile banking Bank Syariah Indonesia tahun 2023? Tujuan penelitian ini adalah Faktor apa saja yang menyebabkan terjadinya pelanggaran privasi data nasabah pada layanan mobile banking tersebut?

Bagaimana langkah mitigasi dan kebijakan yang diterapkan oleh Bank Syariah Indonesia untuk mencegah terulangnya pelanggaran serupa di masa depan? Faktor apa saja yang menyebabkan terjadinya pelanggaran privasi data nasabah pada layanan mobile banking tersebut? Bagaimana langkah mitigasi dan kebijakan yang diterapkan oleh Bank Syariah Indonesia untuk mencegah terulangnya pelanggaran serupa di masa depan? Tujuan Penelitian

Menganalisis bentuk pelanggaran privasi data nasabah akibat serangan siber pada aplikasi mobile banking BSI tahun 2023. Mengidentifikasi faktor penyebab terjadinya pelanggaran privasi data nasabah. Mengevaluasi langkah mitigasi serta kebijakan perlindungan

data yang diterapkan oleh BSI pasca insiden tersebut merupakan hal penting dalam konteks peningkatan keamanan perbankan digital di Indonesia (Otoritas Jasa Keuangan [OJK], 2022). Ruang Lingkup Penelitian ini difokuskan pada kasus serangan siber terhadap aplikasi mobile banking milik Bank Syariah Indonesia (BSI) yang terjadi pada tahun 2023, yang menjadi perhatian nasional karena berdampak pada kepercayaan publik dan stabilitas layanan keuangan digital (Kominfo, 2023). Pembahasan difokuskan pada tiga aspek utama, yaitu: bentuk pelanggaran privasi data nasabah yang terjadi, faktor penyebab pelanggaran, dan upaya mitigasi yang dilakukan oleh pihak bank untuk mengatasi serta mencegah kejadian serupa di masa mendatang, sejalan dengan prinsip manajemen risiko teknologi informasi di sektor perbankan (Basel Committee on Banking Supervision, 2018). Penelitian ini tidak membahas secara teknis sistem enkripsi internal atau arsitektur teknologi perbankan secara mendalam, melainkan lebih menitikberatkan pada analisis keamanan data, perlindungan privasi, serta kebijakan dan etika perbankan digital yang mengatur pengelolaan data nasabah (ISO/IEC, 2019). Ruang lingkup geografis penelitian dibatasi pada lembaga keuangan di Indonesia, dengan fokus utama pada BSI sebagai studi kasus representatif perbankan syariah nasional yang terdampak insiden siber, sesuai dengan kerangka regulasi nasional perlindungan data pribadi (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022).

2. KAJIAN TEORITIS

Pengertian Mobile Banking dan Keamanan Data

Perbankan seluler adalah suatu layanan yang didasarkan pada teknologi digital, memberikan kesempatan kepada pengguna untuk melaksanakan berbagai jenis transaksi lewat perangkat mobile. Fasilitas ini menyediakan kenyamanan, kecepatan, dan efektivitas, tetapi juga menghadirkan isu baru terkait perlindungan data pribadi pengguna. Menurut Rahmahdhani et al. (2022), kemajuan dalam digitalisasi perbankan sangat terkait dengan meningkatnya potensi kebocoran data. Tursinah et al. (2024) pun mengungkapkan bahwa tingkat keamanan informasi yang tinggi dapat mempengaruhi kepercayaan dan kepuasan pengguna terhadap layanan perbankan seluler.

Pelanggaran Privasi Data Nasabah

Pelanggaran atas privasi data nasabah terjadi saat data pribadi seperti identifikasi, akun, atau riwayat transaksi dimanfaatkan tanpa persetujuan. Irmawati dan tim (2024) mengemukakan bahwa meskipun hukum mengenai perlindungan data pribadi telah diatur dalam UU Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi, implementasinya dalam industri perbankan masih mengalami banyak tantangan. Hal ini didukung oleh hasil

penelitian Antoine dan rekan-rekannya (2023) yang menunjukkan bahwa penyebab utama kebocoran data berasal dari lemahnya penerapan kebijakan keamanan dan kurangnya kesadaran pegawai dalam melindungi kerahasiaan informasi digital.

Ancaman Siber dan Kasus BSI

Ancaman dunia maya seperti ransomware, phishing, dan malware menjadi tantangan utama yang sering dihadapi oleh sektor perbankan digital. Salah satu insiden besar yang menarik perhatian publik adalah serangan dunia maya yang menargetkan Bank Syariah Indonesia (BSI) pada bulan Mei 2023. Kumpulan peretas yang dikenal sebagai LockBit 3.0 diduga berhasil mencuri data sebanyak 1,5 terabita yang berisi rincian pribadi dari jutaan nasabah (Kompas. id, 2023). Penelitian yang dilakukan oleh Aziza dan Wardhani (2023) menunjukkan bahwa sejumlah aplikasi mobile banking di Indonesia masih memiliki kelemahan dalam aspek keamanan, terutama pada sistem autentikasi dan enkripsi data, yang membuat bank tersebut rentan terhadap serangan yang serupa.

Regulasi dan Upaya Mitigasi

Perlindungan untuk data pribadi di Indonesia telah diatur dalam Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022, yang mewajibkan lembaga keuangan untuk memastikan keamanan serta kerahasiaan informasi milik nasabah. Firdaus dan rekan-rekan (2023) merekomendasikan agar bank meningkatkan sistem keamanan mereka melalui penerapan enkripsi, melakukan audit secara berkala, serta menerapkan pengawasan internal yang ketat. Dalam hal perbankan syariah, Ardiansyah dan rekan-rekan (2023) mengungkapkan bahwa sektor ini masih perlu melakukan perbaikan pada kesiapan infrastruktur teknologi informasi agar mampu mengatasi ancaman digital dengan cara yang lebih optimal dan sebanding dengan bank-bank konvensional.

Kerangka Pemikiran Penelitian

Berdasarkan kajian literatur sebelumnya, studi ini dibangun atas pemahaman bahwa keamanan informasi memiliki peranan krusial dalam melindungi privasi pengguna mobile banking. Pelanggaran terhadap privasi umumnya terjadi akibat kelemahan pada sistem keamanan, kurangnya kesadaran di kalangan pengguna, serta penerapan regulasi yang belum optimal. Peristiwa kebocoran data yang terjadi pada BSI menjadi ilustrasi nyata bahwa ancaman siber tetap merupakan resiko yang signifikan bagi perbankan digital di Indonesia. Oleh sebab itu, penelitian ini menekankan pentingnya penguatan perlindungan data pribadi serta peningkatan kebijakan keamanan di sektor perbankan, khususnya pada layanan mobile banking yang berbasis syariah.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif, karena bertujuan untuk menggambarkan dan menganalisis secara mendalam fenomena pelanggaran privasi data pada layanan mobile banking. Pendekatan kualitatif dianggap paling relevan untuk memahami konteks sosial, teknologi, dan kebijakan yang melatarbelakangi insiden serangan siber terhadap Bank Syariah Indonesia (BSI) pada tahun 2023. Menurut Sugiyono (2019), penelitian kualitatif digunakan untuk meneliti kondisi objek alamiah di mana peneliti menjadi instrumen utama, serta hasilnya lebih menekankan pada makna daripada generalisasi. Dengan demikian, pendekatan ini dapat membantu peneliti memahami secara komprehensif isu keamanan data dan dampaknya terhadap kepercayaan nasabah. Adapun batasan penelitian ini difokuskan pada kasus pelanggaran privasi data yang terjadi akibat serangan siber terhadap Bank Syariah Indonesia pada tahun 2023. Pembahasan penelitian difokuskan pada aspek keamanan sistem, kebijakan perlindungan data, serta dampaknya terhadap kepercayaan nasabah. Penelitian ini tidak membahas aspek finansial maupun teknis pemrograman secara mendalam, melainkan menitikberatkan pada analisis kebijakan dan implikasi sosial dari insiden kebocoran data tersebut.

4. HASIL DAN PEMBAHASAN

Gambaran Umum Kasus Pelanggaran Privasi pada Mobile Banking BSI

Kasus pelanggaran privasi data yang dialami oleh Bank Syariah Indonesia (BSI) pada bulan Mei 2023 menjadi salah satu kejadian siber paling signifikan dalam dunia perbankan di tanah air. Menurut informasi dari Kompas (2023) dan Tempo (2023), kelompok peretas global bernama LockBit 3.0 mengklaim telah melakukan pencurian sekitar 1,5 terabita data dari infrastruktur BSI. Data yang diambil diduga mencakup informasi pribadi pelanggan, catatan transaksi, serta dokumen internal bank. Serangan ini menyebabkan layanan mobile banking BSI mengalami gangguan selama beberapa hari, yang berakibat pada terhambatnya aktivitas keuangan ribuan nasabah di seluruh Indonesia. Dampak langsung dari peristiwa ini bukan hanya terlihat pada gangguan operasional, tetapi juga berpengaruh pada menurunnya tingkat kepercayaan masyarakat terhadap keamanan data dalam sektor perbankan digital.

Analisis Faktor Penyebab Pelanggaran Privasi

Hasil kajian terhadap dokumen dan wawancara dengan pihak terkait menunjukkan bahwa pelanggaran privasi data di BSI disebabkan oleh beberapa faktor yang saling berkaitan. Faktor pertama adalah kelemahan pada sistem keamanan internal, dikarenakan pembaruan sistem (patch update) yang tidak dilakukan secara konsisten, sehingga muncul celah yang bisa

dimanfaatkan oleh pihak yang tidak bertanggung jawab. Faktor kedua adalah sistem enkripsi yang belum sepenuhnya mengimplementasikan mekanisme end-to-end, sehingga data yang dikirimkan lebih rentan untuk disadap. Faktor ketiga adalah kurangnya deteksi awal terhadap ancaman siber, karena sistem pemantauan keamanan belum beroperasi dengan baik. Selain itu, rendahnya kesadaran terhadap keamanan data dari pengguna dan staf internal juga memperburuk keadaan. Penelitian oleh Aziza dan Wardhani (2023) menemukan bahwa sebagian besar aplikasi mobile banking di Indonesia masih memiliki kelemahan dalam sistem autentikasi dan perlindungan data pribadi pengguna, sehingga risiko pelanggaran serupa bisa terjadi di berbagai institusi keuangan lainnya.

Tindakan dan Respons Bank Syariah Indonesia

Menanggapi serangan itu, BSI telah mengambil berbagai tindakan strategis untuk mengurangi efeknya. Bank segera melakukan peninjauan terhadap keamanan internal dengan melakukan audit untuk mengevaluasi seluruh sistem digitalnya. Tindakan tersebut disertai dengan penguatan pada firewall serta sistem deteksi ancaman otomatis agar dapat mengenali serangan dengan lebih cepat di masa yang akan datang. Selain itu, BSI bekerja sama dengan Badan Siber dan Sandi Negara untuk membantu dalam pemulihan dan penyelidikan. Pihak manajemen juga menjaga komunikasi terbuka dengan masyarakat melalui konferensi pers dan saluran digital resmi, untuk mempertahankan kepercayaan nasabah. Keterbukaan ini diiringi dengan program edukasi tentang keamanan digital guna meningkatkan kesadaran pengguna. Meskipun pemulihan sistem dan reputasi memerlukan waktu, langkah-langkah cepat yang diambil BSI dianggap berhasil dalam memperoleh kembali sebagian kepercayaan publik terhadap layanan mobile banking mereka.

Dampak Sosial dan Reputasi terhadap BSI

Implikasi sosial dari insiden ini cukup besar. Banyak pelanggan merasa cemas akan kebocoran informasi pribadi mereka dan menjadi lebih waspada dalam memanfaatkan layanan daring. Nama baik BSI sempat merosot, terutama di platform media sosial di mana banyak pembicaraan mengenai masalah keamanan data. Namun, respons cepat dan keterbukaan dari pihak manajemen berhasil mengurangi krisis kepercayaan yang mungkin semakin parah. Insiden ini juga menumbuhkan kesadaran baru di masyarakat tentang betapa pentingnya keamanan digital dalam transaksi keuangan. Sebagian pelanggan bahkan mulai menerapkan kebiasaan baru seperti rutin mengganti password dan menghindari akses aplikasi melalui jaringan publik. Dari perspektif organisasi, kejadian ini menjadi kesempatan bagi BSI untuk memperkuat infrastruktur keamanan digitalnya serta meningkatkan kemampuan personel dalam bidang teknologi informasi dan keamanan siber.

Pembahasan dan Implikasi Penelitian

Temuan dari penelitian ini mengindikasikan bahwa isu pelanggaran privasi data dalam layanan perbankan mobile bukan hanya terkait dengan faktor teknis, tetapi juga dipengaruhi oleh kebijakan internal serta perilaku para pengguna. Dari segi teknologi, alangkah pentingnya memiliki sistem keamanan yang terintegrasi dengan pemeliharaan yang rutin dan kemampuan untuk mendeteksi ancaman secara langsung. Dalam hal kebijakan, penerapan Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) harus dijadikan dasar dalam menyusun standar operasional untuk melindungi data di setiap institusi finansial. Sementara itu, dari perspektif pendidikan, peningkatan pemahaman digital di kalangan masyarakat menjadi suatu keharusan agar para nasabah dapat mengerti tanggung jawab mereka dalam menjaga keamanan data pribadi. Oleh sebab itu, pencegahan pelanggaran privasi di masa depan memerlukan pendekatan yang melibatkan berbagai disiplin ilmu, yang menghubungkan aspek teknologi, regulasi, dan kesadaran pengguna. Strategi ini tidak hanya memperkuat perlindungan data, tetapi juga menciptakan ekosistem digital yang lebih aman dan berkelanjutan bagi semua pengguna layanan keuangan digital di Indonesia.

5. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa pelanggaran privasi data nasabah pada aplikasi mobile banking Bank Syariah Indonesia (BSI) tahun 2023 terjadi akibat serangan siber ransomware yang memanfaatkan kelemahan sistem keamanan internal, keterlambatan pembaruan sistem, serta rendahnya kesadaran keamanan digital. Insiden ini berdampak pada gangguan layanan dan menurunnya kepercayaan nasabah, sehingga menunjukkan bahwa perlindungan data pribadi dalam perbankan digital memerlukan penguatan teknologi, kebijakan yang konsisten, serta peningkatan literasi keamanan sesuai dengan Undang-Undang Perlindungan Data Pribadi.

Saran

Bank Syariah Indonesia disarankan untuk terus meningkatkan sistem keamanan digital melalui pembaruan sistem secara berkala, penerapan enkripsi yang lebih kuat, serta peningkatan pengawasan keamanan siber. Selain itu, edukasi keamanan digital bagi karyawan dan nasabah perlu diperkuat, serta peran pemerintah dan regulator diharapkan lebih optimal dalam mengawasi penerapan perlindungan data agar kejadian serupa tidak terulang di masa mendatang.

DAFTAR REFERENSI

Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2023). Penyalahgunaan data pribadi dalam teknologi transaksi digital di industri perbankan digital: Studi kasus PT Bank Syariah Indonesia. *Jurnal Multidisiplin Ilmu Akademik*.

Cahyono, D., Fahrudin, R., Alwiyah, A., & Sinclair, A. (2023). Pentingnya edukasi dalam mengatasi keamanan data mobile banking di Indonesia. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi, 3*(1), 81-89.

Dengan format ini, referensi sudah terstruktur sesuai dengan gaya APA, dan DOI tetap dipertahankan di bagian yang relevan.

Firdaus, S. E., Hidayah, S., & Putro, H. (2023). Implementasi teknologi untuk penguatan keamanan data pribadi nasabah dalam sektor perbankan. *Jurnal Ilmiah Nusantara, 2*(1).

Hutagaol, B. J., Sitorus, R. S., & Hutagaol, N. (2024). Identifikasi tingkat kesadaran pengguna mobile banking terhadap ancaman cybercrime. *Jurnal Teknologi Sistem Informasi dan Aplikasi, 7*(3). https://doi.org/10.32493/jtsi.v7i3.41639

Hutagaol, B. J., Sitorus, R. S., & Hutagaol, N. (2024). Identifikasi tingkat kesadaran pengguna mobile banking terhadap ancaman cybercrime. *Jurnal Teknologi Sistem Informasi dan Aplikasi, 7*(3), 1043-1054. https://doi.org/10.32493/jtsi.v7i3.41639

ISO/IEC. (2019). *ISO/IEC 27001:2019 Information security management systems*. International Organization for Standardization.

Judijanto, L., Ariyanti, R., & Suryani, S. (2024). Analysis of the impact of mobile banking technology, fintech, and digital transaction security on customer loyalty at BUMN banks in Indonesia. *West Science Social and Humanities Studies, 2*(8), 1299-1309. https://doi.org/10.58812/wsshs.v2i08.1183

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Pernyataan resmi penanganan insiden siber sektor keuangan*.

Lutfi, M. P., Kurniasari, E., & Aida Putri, F. E. (2024). Urgensi perlindungan hukum terhadap data privasi nasabah bank di era perkembangan.

Muliawan, D., & Hasnawati, H. (2023). The influence of cyber security knowledge, cyber security awareness, and behaviour protection on intention to use among mobile banking users in Jakarta. *Jurnal Indonesia Sosial Teknologi*. https://doi.org/10.59141/jist.v5i11.8763

Muliawan, D., & Hasnawati, H. (2024). The influence of cyber security knowledge, cyber security awareness, and behaviour protection on intention to use among mobile banking users in Jakarta. *Jurnal Indonesia Sosial Teknologi, 5*(11), 4904-4916. https://doi.org/10.59141/jist.v5i11.8763

Otoritas Jasa Keuangan. (2022). *POJK Nomor 11/POJK.03/2022 tentang penyelenggaraan teknologi informasi oleh bank umum*.

Priyanto, Z. I., & Indraningsih, N. H. (2024). The impact of end-to-end encryption on the security of digital banking transactions: An in-depth analysis. *Mantik Journal, 8*(3).

Saputri, V. D. (2023). Implementation of biometric-based security system on mobile banking application. *Jurnal Komputer Indonesia, 2*(1), 25-32. https://doi.org/10.37676/jki.v2i1.565

Tursinah, M., Iqbal Fasa, M., & Susanto, I. (2023). Analisis peran keamanan data dalam meningkatkan kepuasan nasabah pada penggunaan mobile banking. *Jurnal Ilmiah Ekonomi, Manajemen dan Syariah*. https://doi.org/10.55883/jiemas.v3i3.87

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Widya Annafa, S., & Simanjuntak, H. P. G. (2021). Tanggung jawab hukum bank dalam kasus kebocoran data nasabah. *Jurnal Multidisiplin Ilmu Akademik, 1*(6). Basel Committee on Banking Supervision. (2018). *Cyber-resilience: Range of practices*. Bank for International Settlements.