

Analisis Perlindungan Data Pribadi Nasabah Perbankan Terhadap Penggunaan Layanan Mobile Banking

Sheila Aida Fitriani¹, Adelia Dara Sasra², Mohammad Harjuno Asmoro Raharjo³

¹²³Universitas Negeri Semarang

Email : sheilaaaida@students.unnes.ac.id¹, adeliadaras@students.unnes.ac.id²,
moharjunoar@students.unnes.ac.id³

Abstract

The Security Of Mobile Banking Is A Concern For Bank Customers Who Use It, Even Though It Can Make Transactions Easier. To Protect Customers From Data Theft, Hacking And Exploitation For Illegal Purposes, Protecting Consumer Data Is Essential. The Author Wants To Investigate How Banking Customers' Personal Information Is Protected When Using Mobile Banking Services, Which Includes Banking Procedures In Protecting Customers' Personal Data Against Mobile Banking Use And The Implementation Of Regulations In Protecting Customers' Personal Data Against Mobile Banking Use In Indonesia. The Personal Data Protection (PDP) Law, Which Provides A Comprehensive Set Of Guidelines For The Processing Of Personal Data In All Sectors, Including Banking. This Research Aims To Examine Laws And Regulations In Indonesia Relating To The Protection Of Personal Information. In This Research, We Used A Normative Study Method Combined With A Conceptual Approach. By Using This Method, Researchers Can Find Out That Collaboration Between The Government, Regulators, Banks And The Community Is The Key To Creating A Safe And Trustworthy Mobile Banking Ecosystem. The Government And Regulators, Such As The Financial Services Authority (OJK) And Bank Indonesia (BI), Need To Continue To Update Regulations To Keep Pace With Technological Developments And Increasingly Complex Cyber Threats.

Abstract

Keamanan mobile banking menjadi kekhawatiran bagi nasabah bank yang menggunakannya, padahal dapat memudahkan transaksi. Untuk melindungi pelanggan dari pencurian data, peretasan, dan eksploitasi untuk tujuan ilegal, perlindungan data konsumen sangatlah penting. Penulis ingin menyelidiki bagaimana informasi pribadi nasabah perbankan dilindungi saat menggunakan layanan mobile banking, yang mencakup prosedur perbankan dalam melindungi data pribadi nasabah terhadap penggunaan mobile banking dan penerapan regulasi dalam melindungi data pribadi nasabah terhadap penggunaan mobile banking di Indonesia. Undang-Undang Perlindungan Data Pribadi (PDP), yang menyediakan seperangkat pedoman komprehensif untuk pemrosesan data pribadi di semua sektor, termasuk perbankan. Penelitian ini bertujuan untuk mengkaji peraturan perundang-undangan di Indonesia yang berkaitan dengan perlindungan informasi pribadi. Dalam Penelitian kali ini, kami menggunakan metode studi normatif dan dikombinasikan dengan pendekatan konseptual. Dengan menggunakan metode ini, peneliti dapat mengetahui bahwa kolaborasi antara pemerintah, regulator, bank, dan masyarakat menjadi kunci untuk menciptakan ekosistem mobile banking yang aman dan terpercaya. Pemerintah dan regulator, seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), perlu terus memperbarui regulasi agar sejalan dengan perkembangan teknologi dan ancaman siber yang semakin kompleks.

Article History

Received Okt 27, 2024
Revised Okt 29, 2024
Accepted 09 Nov 2024
Available online 17 Nov. 2024

Keywords :

Mobile Banking, Protection, Personal Data.

Keywords :

Mobile Banking, Perlindungan, Data Pribadi



<https://doi.org/10.5281/zenodo.14192101>

This is an open-access article under the **CC-BY-SA License**.



PENDAHULUAN

Bank semakin banyak menggunakan teknologi untuk menawarkan layanan swalayan melalui berbagai saluran elektronik. Secara umum, layanan keuangan itu rumit, dan penggunaan teknologi memerlukan kepercayaan yang besar dari pelanggan.¹ seiring dengan semakin majunya teknologi informasi. Banyak bank yang bersemangat mengembangkan ide-ide baru. Untuk menarik perhatian

1 Agung Budiarto and Pujiyono, "Perlindungan Hukum Nasabah Pengguna Mobile Banking," *Jurnal Privat Law* 9, no. Vol 9, No 2 (2021): JULI-DESEMBER (2021): 300–308.

klien, Bank telah mempersiapkan diri dengan mengembangkan fitur keuangan. Mengembangkan layanan keuangan digital, termasuk instrumen pembayaran nontunai dengan kemampuan internet, seluler, dan layanan pesan singkat (SMS) perbankan, menjadi salah satunya. Salah satu produk kemajuan informasi dan teknologi yang dianut oleh industri perbankan adalah mobile banking. Menggunakan telepon seluler untuk mengakses dan memanfaatkan layanan perbankan dikenal sebagai mobile banking. Mengingat mobilitas menjadi prioritas utama kehidupan modern, mobile banking mengalami perkembangan yang sangat pesat. Mobile banking adalah jenis layanan perbankan yang memungkinkan pengguna mengakses informasi keuangan bank mereka melalui ponsel kapan saja, dari lokasi mana saja, sepanjang waktu.²

Salah satu fitur mutakhir yang ditawarkan lembaga keuangan untuk memenuhi kebutuhan konsumen akan akses digital terhadap layanan keuangan melalui beragam fungsi ponsel pintar adalah mobile banking. Nasabah tidak perlu lagi mengunjungi kantor cabang untuk mengakses berbagai layanan penting perbankan, termasuk pembayaran tagihan, transfer tunai antar bank, dan pengecekan saldo rekening, berkat mobile banking. Keleluasaan ini dapat dimanfaatkan oleh nasabah untuk melakukan transaksi perbankan kapanpun dan dimanapun, selama terkoneksi dengan internet, cukup dengan mengetuk beberapa tombol di layar smartphone. Nasabah mendapatkan keuntungan dari kemudahan mobile banking yang tidak hanya menghemat waktu namun juga membuat transaksi menjadi lebih nyaman dan efisien. Karena tata letaknya yang ramah pengguna, aplikasi mobile banking memudahkan orang-orang dari berbagai latar belakang untuk mengakses kemampuan perbankan. Selain membuat layanan lebih mudah diakses, mobile banking merupakan taktik pemasaran baru bagi bank karena memungkinkan mereka terhubung dengan basis klien yang lebih besar, khususnya generasi muda, yang biasanya lebih paham teknologi. Selain itu, karena mobile banking memungkinkan pengguna untuk mengelola dan mengatur rekening mereka tanpa dibatasi oleh waktu dan tempat, hal ini memberikan nilai tambah dalam hal kualitas layanan yang lebih baik. Karena fitur ini, perbankan dapat memberikan pengalaman yang lebih dapat disesuaikan dan mudah disesuaikan kepada nasabah, menjadikan mobile banking sebagai pilihan yang sangat baik di era digital ketika konsumen mencari layanan keuangan yang lebih cepat, nyaman, dan lebih mudah diakses.³

Keamanan mobile banking menjadi kekhawatiran bagi nasabah bank yang menggunakannya, padahal dapat memudahkan transaksi. Menurut Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan Pasal 29 Ayat 4, bank wajib memberitahukan kepada nasabah tentang kemungkinan kerugian yang timbul sehubungan dengan transaksi nasabah yang dilakukan oleh bank untuk kepentingannya. Kajian hukum perbankan ini menjelaskan mengapa nasabah bank mengalami kerugian ketika menggunakan layanan mobile banking. Kerugian ini disebabkan oleh keterlambatan menginformasikan sistem perbankan.⁴ Contoh terkait layanan mobile banking adalah pelanggaran data m-banking pada tahun 2021 yang berdampak pada Bank Negara Indonesia (BNI), salah satu bank besar di negara ini. Di sini, peretas menipu klien agar membocorkan informasi login mereka dengan menggunakan metode phishing. Begitu mereka mendapatkan akses, peretas memindahkan uang dari rekening konsumen ke rekening lain yang sulit dilacak. Nasabah menderita kerugian finansial yang besar akibat peristiwa ini, yang juga memicu kekhawatiran luas terhadap keamanan layanan m-banking di Indonesia. Tingginya frekuensi tuntutan hukum kerusakan properti yang melibatkan mobile banking menunjukkan bahwa perlindungan hukum nasabah bank dalam memanfaatkan mobile banking masih belum memadai.

Kerahasiaan data pelanggan merupakan urusan pribadi yang perlu dijaga dengan baik. Untuk melindungi pelanggan dari pencurian data, peretasan, dan eksploitasi untuk tujuan ilegal, perlindungan data konsumen sangatlah penting. Dari sisi hukum, ketidakmampuan perbankan dalam

2 Dinda Novika Rahmahdhani, Muhammad Irwan Padli Nasution, and Sri Suci Ayu Sundari, "Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking," *JUEB : Jurnal Ekonomi Dan Bisnis* 2, no. 2 (2023): 88–96, <https://doi.org/10.57218/jueb.v2i2.693>.

3 Amania Wahyu Atsari, Kristina Sulatri, and Muhammad Mashuri, "Perlindungan Hukum Bagi Nasabah Perbankan Terhadap Kesalahan Layanan Mobile Banking Dari Sistem Teknologi Informasi Perbankan," *Yurijaya : Jurnal Ilmiah Hukum* 5, no. 1 (2023): 59–72, <https://doi.org/10.51213/yurijaya.v5i1.97>.

4 Rahmahdhani, Nasution, and Sundari, "Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking."

mengantisipasi penggunaan teknologi informasi untuk layanan perbankan melalui program internet banking dan mobile banking bagi nasabah pemilik dana menyebabkan perlindungan data pribadi yang bersifat rahasia tidak dapat diberikan secara maksimal. Bank tidak hanya mengumpulkan data nasabah, tetapi juga mengubahnya menjadi informasi yang dapat digabungkan dari beberapa sumber. Mengingat kondisi teknologi informasi saat ini dan pertumbuhan komunikasi online, semua data pelanggan tersedia untuk diungkapkan kepada publik, pihak berwenang, atau siapa pun yang mungkin tertarik untuk mempelajarinya. Hal ini meningkatkan kemungkinan data disalahgunakan. Masyarakat mengeluhkan kebocoran data pribadi, seperti yang terlihat pada berbagai barang di industri jasa keuangan, yang ditawarkan melalui telepon dan layanan pesan singkat (SMS). Bank mungkin menderita kerugian finansial dan mungkin menurunnya kepercayaan nasabah akibat kejadian ini.⁵

Meskipun tidak ada undang-undang khusus yang mengatur tentang mobile banking di Indonesia, namun terdapat ketentuan yang dapat dimaknai, dijadikan landasan, dan digunakan untuk menentukan perlindungan hukum terhadap nasabah pengguna mobile banking. Salah satu ketentuan tersebut adalah Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan Pasal 29 Ayat (4) yang menyatakan bahwa bank wajib memberitahukan kepada nasabah mengenai potensi risiko kerugian atas transaksi yang dilakukan atas nama nasabah. Mengingat latar belakang ini, penulis ingin menyelidiki bagaimana informasi pribadi nasabah perbankan dilindungi saat menggunakan layanan mobile banking, yang mencakup Bagaimana prosedur perbankan dalam melindungi data pribadi nasabah terhadap penggunaan mobile banking? dan Bagaimana penerapan regulasi dalam melindungi data pribadi nasabah terhadap penggunaan mobile banking di Indonesia? dengan maksud untuk mengkaji peraturan perundang-undangan di Indonesia yang berkaitan dengan perlindungan informasi pribadi, khususnya yang mengatur penggunaan data klien dalam layanan mobile banking.

METODE PENELITIAN

Dalam Penelitian kali ini, kami mengkombinasikan metode yuridis normatif dan dengan pendekatan konseptual. Metode yuridis normatif yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur yang berkaitan dengan permasalahan yang diteliti. Sedangkan untuk pendekatan konseptual dimaksudkan untuk menganalisa bahan hukum melalui literatur, buku, dan artikel terkait dengan topik yang dibahas, sehingga dapat diketahui makna yang terkandung pada istilah-istilah hukum. Hal itu dilakukan sebagai usaha untuk memperoleh makna baru yang terkandung dalam istilah-istilah yang diteliti, atau menguji istilah hukum tersebut dalam teori dan praktek. Dengan menggabungkan kedua metode ini, kita dapat mengembangkan pemahaman mendalam terkait permasalahan ini, baik dari perspektif normatif maupun teoritis.

HASIL DAN PEMBAHASAN

1. Prosedur Perbankan Dalam Melindungi Data Pribadi Nasabah Terhadap Penggunaan Mobile Banking

Menurut UU No. 10 Tahun 1998, bank adalah lembaga yang bertugas menghimpun dana dari masyarakat dan menyalurkannya kembali dalam bentuk kredit atau manfaat lainnya. Industri perbankan telah mengalami revolusi digital yang signifikan seiring dengan pesatnya kemajuan teknologi informasi. Salah satu inisiatif bank untuk menjawab kebutuhan nasabahnya yang terus berubah dan kompleks adalah penerapan layanan perbankan digital seperti internet banking, *mobile banking* (*M-Banking*), dan SMS banking.⁶ Penyelenggaraan layanan perbankan digital oleh bank umum diatur dalam Peraturan OJK No. 12/POJK.03/2018 yang menyebutkan bahwa “layanan perbankan digital merupakan layanan perbankan secara elektronik yang dikembangkan dengan mengoptimalkan pemanfaatan data nasabah dalam rangka melayani nasabah secara lebih cepat, mudah, dan sesuai kebutuhan (*customer experience*), serta dapat dilaksanakan sepenuhnya

5 Ema Irmawati, John Pieries, and Wiwik Sri Widiarty, “PERLINDUNGAN HUKUM ATAS DATA PRIBADI NASABAH BANK PENGGUNA MOBILE BANKING DALAM PERSPEKTIF UU NO 27 TAHUN 2022 TENTANG KEBOCORAN DATA,” *Syntax Admiration* 15, no. 1 (2024): 37–48.

6 Rahmahdhani, Nasution, and Sundari, “Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking.”

oleh nasabah secara mandiri, dengan tetap memperhatikan aspek keamanan.”⁷ OJK mendefinisikan m-banking sebagai layanan perbankan yang dapat diakses kapan saja dan dari mana saja, serta dilakukan melalui perangkat seluler. Tujuan M-Banking adalah untuk memudahkan masyarakat umum dalam melakukan berbagai transaksi keuangan. Nasabah dapat menggunakan teknologi seluler untuk mengakses berbagai kemampuan perbankan dengan memasang program di perangkat mereka.⁸

Keamanan informasi dan data adalah proses mencegah informasi agar tidak hilang, diubah, atau diungkapkan baik secara sengaja maupun tidak sengaja—dengan bantuan hukum dan teknologi. Mengetahui data apa yang Anda miliki, di mana data tersebut berada, dan mengenali bahaya data merupakan bagian dari keamanan data. Mencegah kerusakan material, menurunkan risiko penyalahgunaan data, dan menurunkan kemungkinan aktivitas kriminal merupakan tiga tujuan utama keamanan data. Mengingat peningkatan tajam dalam pencurian data, perlindungan data menjadi sangat penting. Keamanan data membantu dalam memahami konteks operasi pengguna dan data, mencegah penggunaan data yang tidak sah, serta mengidentifikasi dan mengurangi bahaya data.⁹

Beberapa lapisan perlindungan merupakan dasar dari model yang saat ini digunakan dalam sistem perbankan online, yang terdiri dari beberapa metode dan prosedur paralel yang dirancang untuk menyediakan identitas, autentikasi, dan otorisasi sekaligus menjaga keamanan aplikasi perbankan dan data pengguna. Berikut ini adalah contoh model sistem perbankan online:¹⁰

1. **Digital Certificate**

Dengan menjamin autentikasi pengguna dan sistem, sertifikat digital meningkatkan keamanan transaksi keuangan. Infrastruktur kunci publik (PKI) yang menggunakan pihak ketiga yang andal untuk mengonfirmasi identitas mendukung prosedur ini.

2. **One Time Password Tokens**

Sebagai lapisan keamanan tambahan, perangkat OTP berfungsi sebagai metode autentikasi kedua. Karena data yang dicuri tidak dapat digunakan lagi, OTP menghentikan serangan siber dengan membuat kata sandi sekali pakai yang terus berubah.

3. **One Time Password Cards**

Meskipun kartu OTP menyediakan opsi autentikasi dua faktor yang lebih hemat biaya, kekurangannya adalah kemungkinan kata sandi yang dihasilkan digunakan dalam lebih dari satu transaksi. Karena itu, sistem rentan terhadap serangan yang sering terjadi dalam waktu yang singkat.

4. **Browser Protection**

Dengan melindungi browser yang digunakan untuk mengakses sistem, keamanan sistem akan meningkat. Untuk mengidentifikasi dan menghentikan serangan malware yang menargetkan data pribadi pengguna, browser dipantau.

5. **Virtual Keyboards**

Keyboard virtual memanfaatkan kriptografi dan teknologi Java untuk melawan ancaman keylogger. Dengan cara ini, data yang dimasukkan langsung dienkripsi, sehingga menyulitkan perangkat lunak pengawasan untuk memperoleh informasi pribadi.

6. **Device Registering**

Dengan membatasi akses ke sistem keuangan pada perangkat yang telah diverifikasi dengan pemindaian sidik jari, teknik ini meningkatkan keamanan. Perangkat yang tidak terdaftar tidak akan dapat mengakses akun.

7. **CAPTCHA**

7 Herdian Ayu Andreana Beru Tarigan and Darminto Hartono Paulus, “Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital,” *Jurnal Pembangunan Hukum Indonesia* 1, no. 3 (2019): 294–307, <https://doi.org/10.14710/jphi.v1i3.294-307>.

8 Lidia Sihotang and Ilham Hudi, “Penerapan M-Banking Dalam Meningkatkan Jasa, Layanan Perbankan Di Bank Rakyat Indonesia Kantor Cabang Pekanbaru Sudirman,” *Jurnal Akuntansi AKTIVA* 4, no. 2 (2023): 106–14, <https://doi.org/10.24127/akuntansi.v4i2.4831>.

9 Rohid Akbar, Muhammad Irwan, and Padli Nasution, “Journal of Sharia Economics Scholar (JoSES) Analisis Keamanan Data Pada Aplikasi Mobile Banking Journal of Sharia Economics Scholar (JoSES)” 2, no. 2 (2024): 79–83.

10 Rahmahdhani, Nasution, and Sundari, “Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking.”

Manusia dan komputer dapat dibedakan menggunakan CAPTCHA. Untuk menghentikan robot melakukan aktivitas daring yang berbahaya, CAPTCHA memberikan tugas yang menantang kepada komputer, seperti menguraikan gambar yang tidak jelas.

8. Short Message Service (SMS)

Dengan memberikan kode verifikasi kepada pengguna, teknik ini memungkinkan autentikasi dua faktor dan menjamin bahwa transaksi dimulai oleh pengguna yang valid.

9. Device Identification

Model identifikasi ini mengenali dan memberikan akses kepada pengguna dengan menggunakan atribut fisik perangkat. Model ini dapat digunakan sebagai solusi mandiri untuk meningkatkan keamanan akses perbankan online, serta sebagai pelengkap langkah-langkah keamanan lainnya.

10. Positive Identification

Teknik verifikasi identitas yang dikenal sebagai "identifikasi positif" meminta pengguna untuk mengungkapkan informasi pribadi yang hanya diketahui oleh orang tersebut. Setelah kata sandi, data ini bertindak sebagai faktor autentikasi kedua.

11. Pass-Phrase

Untuk mengonfirmasi identitas pengguna selama transaksi keuangan, teknik keamanan ini bergantung pada informasi pribadi yang berbeda. Teknik ini berfungsi sebagai tindakan pengamanan tambahan selain kata sandi.

12. Transaction Monitoring

Banyak sistem perbankan online yang menggunakan paradigma keamanan ini. Untuk menemukan pola transaksi yang berpotensi sebagai *fraud*, setiap bank menggunakan serangkaian metode yang berbeda, mulai dari analisis transaksi historis hingga kecerdasan buatan..

13. Secure Socket Layer (SSL)

Teknologi umum yang disebut Secure Socket Layer (SSL) digunakan untuk mengamankan komunikasi internet. SSL berfungsi sebagai tingkat perlindungan ekstra untuk informasi pribadi kita saat kita mengunjungi dan menggunakan situs web bank untuk perbankan online. Data dienkripsi oleh SSL, yang mengubahnya menjadi kode yang hanya dapat diuraikan oleh komputer kita dan server bank.

14. Token (One-Time Password Tokens)

Perangkat yang membuat kata sandi sekali pakai untuk memverifikasi transaksi perbankan daring dikenal sebagai token atau kalkulator keamanan. Token tersebut perlu diaktifkan dengan memasukkan kata sandi pribadi sebelum dapat digunakan. Oleh karena itu, token tersebut melindungi rekening bank kita dengan menambahkan tingkat keamanan lain.

Untuk melindungi data privasi nasabah dalam layanan *M-Banking*, bank biasanya memiliki sistem yang memiliki kemampuan unik untuk memutus koneksi ke server *M-Banking*. Jika pengguna aplikasi tidak melakukan apa pun selama minimal dua menit, server akan secara otomatis keluar, dan pengguna harus memasukkan kembali kata sandi mereka saat kembali ke aplikasi *M-Banking*.¹¹

Dalam melindungi informasi pribadi nasabah *M-Banking*, bank menggunakan sistem keamanan berlapis yang terdiri dari beberapa solusi dan metode yang dilakukan secara bersamaan. Menyediakan fitur autentikasi transaksi, yang mengharuskan pengguna untuk mengonfirmasi identitas mereka menggunakan kombinasi login, kata sandi, dan kata sandi sekali pakai (OTP) yang dikirim melalui SMS ke nomor telepon yang terdaftar, merupakan salah satu cara bank mengamankan layanan *M-Banking* mereka. Karena tidak memiliki akses langsung, peretas akan merasa lebih sulit untuk membobol akun *M-Banking* pengguna berkat fitur OTP ini. Selain itu, bank terus-menerus menghimbau nasabah—termasuk teller dan layanan nasabah—

11 Hanafittya, "ANALISIS PERLINDUNGAN KERAHASIAAN DATA PRIBADI PADA NASABAH PENGGUNA PRODUK LAYANAN MOBILE BANKING BANK MILIK THE ANALYSIS OF THE SECURITY PROTECTION OF PRIVACY DATA ON THE CUSTOMER OF MOBILE BANKING SERVICE PRODUCT IN ACEH PROVINCIAL PENDAHULUAN Bank Mil," *Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan* 5, no. 2 (2021): 328–37.

untuk tidak membocorkan kode OTP. Dengan menggunakan kode OTP ini, setiap transaksi dapat dijamin memerlukan persetujuan nasabah. (DBS 2021) Pembuatan kode keamanan merupakan fitur keamanan lain yang ditawarkan oleh layanan *M-Banking* yang membantu memastikan privasi dan keamanan identitas, uang, dan transaksi pengguna. Berikut ini merupakan kode keamanan untuk layanan *M-Banking*:¹²

a. Personal Identification Number (PIN)

Suatu kode yang berisikan untaian angka, biasanya terdiri dari 6 digit numerik, yang dapat digunakan pemegang kartu sebagai kata sandi untuk mengakses sistem perbankan dan melakukan transaksi menggunakan ATM, Internet Banking, *M-Banking*, ataupun sistem akses lainnya yang ditentukan oleh bank.

b. Mobile Personal Identification Number (M-PIN)

kata sandi atau kode yang unik bagi nasabah dan digunakan untuk mengotorisasi transaksi perbankan di *M-Banking*.

c. Kode Aktivasi

Sebagai bagian dari prosedur registrasi pertama melalui aplikasi layanan *M-Banking*, kode rahasia yang dibuat oleh sistem bank dikirimkan ke telepon pintar milik nasabah yang telah terdaftar di sistem bank. Tujuan dari kode ini adalah untuk memverifikasi keakuratan data pendaftar.

d. User ID

Identitas yang dimiliki oleh nasabah yang dimasukkan setiap kali mereka mengakses atau menggunakan layanan *M-Banking*.

Lebih jauh lagi, beberapa bank telah menambahkan tingkat perlindungan ekstra dengan menerapkan teknologi biometrik, seperti sidik jari atau pengenalan wajah, untuk menjamin bahwa hanya pemegang rekening yang sah yang dapat menggunakan layanan *M-Banking*. Bank menggunakan teknologi enkripsi ujung ke ujung dengan standar industri terkini untuk menjaga keamanan transaksi dan data yang ditransfer. Protokol SSL/TLS (Secure Socket Layer/Transport Layer Security) digunakan untuk mengenkripsi semua data yang dipertukarkan antara server bank dan aplikasi *M-Banking*, dengan tingkat enkripsi minimum 256 bit. Untuk memperbaiki potensi kerentanan baru, bank juga secara berkala memperbarui sistem keamanan dan patch mereka. Bank juga menggunakan sistem pemantauan waktu nyata untuk menemukan kemungkinan pelanggaran keamanan dan aktivitas yang tidak biasa.

Keadaan tak terduga (insiden) yang diakibatkan oleh penyalahgunaan, aktivitas kriminal, dan/atau situasi mendesak dapat muncul saat layanan *M-Banking* diberikan. Peristiwa yang sangat meningkatkan risiko dianggap sebagai peristiwa kritis. Penyalahgunaan teknologi informasi atau aktivitas kriminal didefinisikan sebagai aktivitas apa pun yang mengakibatkan kerugian moneter atau mengganggu kemampuan bank untuk beroperasi secara efisien. Oleh karena itu, peraturan berikut mengatur cara penanganan kejadian insidental:¹³

- Unit kerja (Divisi, Kantor Cabang, Kantor Cabang Pembantu, dan Kantor Kas) yang menemukan penyalahgunaan wajib menyampaikan temuannya kepada Teknologi Informasi untuk ditindaklanjuti apabila Bank menemukan penyalahgunaan atau tindak pidana akibat dari kelemahan sistem teknologi informasi.
- Unit kerja yang menerima laporan harus meneruskannya ke Divisi Produk dan Layanan di Sektor Perlindungan Pelanggan untuk ditindaklanjuti jika nasabah menemukan penyalahgunaan atau aktivitas ilegal. Untuk meminimalkan dan mengurangi dampak risiko yang ditimbulkan, penyelesaian kasus harus dikoordinasikan dengan Divisi terkait.
- Setiap penyalahgunaan atau aktivitas ilegal yang melibatkan teknologi *M-Banking* harus dilaporkan kepada OJK, sesuai dengan Surat Edaran OJK No: 12/SEOJK.03/2017 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

Protokol yang ketat dipatuhi dalam pengelolaan dan penyimpanan data nasabah sesuai dengan hukum yang berlaku. Informasi nasabah yang sensitif disimpan di pusat data dengan keamanan

¹² Hanafitty.

¹³ Hanafitty.

tinggi di server yang dilindungi oleh firewall canggih. Hanya pegawai bank yang berwenang yang memiliki akses ke data tersebut, yang diawasi ketat oleh sistem manajemen log. Namun, bank-bank di Indonesia tidak akan dimintai pertanggungjawaban atau menawarkan kompensasi apa pun atas segala kerusakan, klaim, atau litigasi yang mungkin ditimbulkan oleh nasabah atau pihak lain sebagai akibat dari kecerobohan mereka saat menggunakan layanan *M-Banking*. Hal ini menyoroti betapa pentingnya bagi pengguna layanan *M-Banking* untuk selalu berhati-hati dan mematuhi langkah-langkah keamanan yang ditetapkan.

2. Penerapan Regulasi Dalam Melindungi Data Pribadi Nasabah Terhadap Penggunaan Mobile Banking di Indonesia

Perlindungan data pribadi dalam perbankan seluler menjadi semakin penting di Indonesia, mengingat pesatnya pertumbuhan layanan keuangan digital. Bab pembahasan ini bertujuan untuk memberikan analisis komprehensif tentang kerangka regulasi dan penerapannya dalam melindungi data pribadi nasabah perbankan seluler di Indonesia. Indonesia telah menetapkan kerangka regulasi yang kuat untuk mengatasi tantangan perlindungan data pribadi di era digital, dengan implikasi khusus bagi sektor perbankan seluler. Landasan kerangka ini adalah Undang-Undang Perlindungan Data Pribadi (PDP), yang disahkan sebagai Undang-Undang No. 27 Tahun 2022, yang menyediakan seperangkat pedoman komprehensif untuk pemrosesan data pribadi di semua sektor, termasuk perbankan.

Undang-undang ini terinspirasi dari standar internasional seperti Peraturan Perlindungan Data Umum (GDPR) Uni Eropa, yang menandakan komitmen Indonesia untuk menyelaraskan dengan praktik terbaik global dalam perlindungan data. UU PDP memperkenalkan prinsip-prinsip penting yang mengatur pemrosesan data pribadi, termasuk keabsahan, keadilan, transparansi, pembatasan tujuan, minimalisasi data, keakuratan, dan integritas. Prinsip-prinsip ini khususnya relevan dengan perbankan seluler, di mana sejumlah besar data keuangan sensitif diproses setiap hari. Bank dan lembaga keuangan yang menawarkan layanan perbankan seluler kini harus memastikan bahwa aktivitas pemrosesan data mereka mematuhi prinsip-prinsip ini, yang pada dasarnya mengubah pendekatan mereka terhadap pengelolaan data nasabah. Melengkapi UU PDP adalah UU Informasi dan Transaksi Elektronik (ITE) yang awalnya diundangkan melalui UU No. 11 Tahun 2008 dan kemudian diubah dengan UU No. 19 Tahun 2016. Undang-undang ini sangat penting untuk perbankan seluler karena mengatur transaksi dan informasi elektronik, menyediakan lapisan perlindungan tambahan untuk data pribadi dalam lingkungan digital. Ketentuan Undang-Undang EIT sangat penting dalam membangun kerangka hukum untuk transaksi elektronik yang aman, yang menjadi tulang punggung layanan perbankan seluler.¹⁴

a. Peraturan Khusus Sektor

Meskipun UU PDP dan UU ITE memberikan kerangka kerja yang luas untuk perlindungan data, sektor perbankan tunduk pada peraturan khusus sektor tertentu yang semakin memperkuat perlindungan data pribadi dalam perbankan seluler. Otoritas Jasa Keuangan (OJK) memainkan peran penting dalam hal ini, dengan mengeluarkan peraturan yang berdampak langsung pada praktik perlindungan data di sektor keuangan. Salah satu contohnya adalah Peraturan OJK No. 6/POJK.07/2022 tentang Perlindungan Konsumen dan Perlindungan Masyarakat di Sektor Jasa Keuangan yang mengamanatkan penyelenggaraan sistem teknologi informasi yang andal untuk melindungi data konsumen. Peraturan ini menggarisbawahi pentingnya perlindungan teknologi dalam memastikan integritas dan kerahasiaan data pribadi di platform perbankan seluler.¹⁵ Lebih lanjut, Peraturan OJK Nomor 12/POJK.03/2016 Tentang Penyelenggaraan Layanan Digital Oleh Bank Indonesia. Peraturan difokuskan pada penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum yang berimplikasi langsung pada layanan mobile banking. Peraturan ini

¹⁴ Danil Erlangga Mahameru et al., "Implementasi Uu Perlindungan Data" 5, no. 20 (2023): 115–31.

¹⁵ Jurnal Kajian et al., "Perlindungan Hukum Preventif Oleh Ojk Dalam Mencegah Kebocoran Data Pribadi Konsumen Pinjaman Online Berdasarkan Peraturan Ojk Nomor 06/Pojk.07/2022 Tentang Perlindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan," *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan* 3 (2023): 1–9.

mengharuskan bank untuk mengadopsi praktik manajemen risiko yang komprehensif, termasuk yang terkait dengan perlindungan data, dalam operasi perbankan digital mereka.¹⁶

b. Tantangan dan Praktik Implementasi

Penerapan peraturan ini di sektor perbankan seluler menghadirkan tantangan sekaligus peluang bagi lembaga keuangan. Bank diharuskan mengadopsi pendekatan multi-aspek terhadap perlindungan data, yang mencakup langkah-langkah teknologi, prosedural, dan hukum. Salah satu syarat utama adalah penerapan prosedur Know Your Client (KYC), yang sangat penting tidak hanya untuk mencegah kejahatan keuangan tetapi juga untuk memastikan integritas dan keakuratan data nasabah. Prosedur ini melibatkan proses identifikasi, verifikasi, dan pemantauan yang ketat, yang khususnya menantang dalam konteks perbankan seluler di mana interaksi tatap muka terbatas.

Bank juga memanfaatkan teknologi canggih untuk meningkatkan perlindungan data. Misalnya, studi kasus bank terkemuka di Indonesia mengungkapkan keberhasilan penerapan Thales CipherTrust untuk melindungi data nasabah dan memastikan kepatuhan terhadap persyaratan peraturan. Contoh ini menunjukkan bagaimana bank secara proaktif mengadopsi solusi enkripsi dan perlindungan data yang canggih untuk melindungi informasi sensitif dalam menghadapi ancaman dunia maya yang terus berkembang. Solusi pembelajaran mesin juga digunakan oleh beberapa bank swasta terbesar di Indonesia untuk meningkatkan keamanan layanan perbankan digital. Teknologi canggih ini tidak hanya melindungi data nasabah tetapi juga selaras dengan standar keamanan global, yang menunjukkan komitmen sektor perbankan untuk selalu unggul dalam menghadapi potensi risiko keamanan.¹⁷

c. Pengawasan dan Penegakan Peraturan

Penerapan regulasi perlindungan data yang efektif dalam mobile banking diawasi oleh banyak badan regulator. Kementerian Komunikasi dan Informatika (Menkominfo) memegang peranan penting dalam menegakkan undang-undang perlindungan data yang terkait dengan data elektronik, termasuk pendaftaran operator sistem elektronik seperti bank yang menyediakan layanan digital. Otoritas Jasa Keuangan (OJK) melengkapi pengawasan ini dengan memastikan lembaga keuangan mematuhi standar perlindungan data dan undang-undang perlindungan konsumen khusus untuk sektor perbankan. Mekanisme pengawasan ganda ini membantu menciptakan lingkungan regulasi komprehensif yang membahas aspek teknologi dan keuangan dari perlindungan data perbankan seluler.

Pengawasan dan penegakan aturan perbankan memiliki peran penting dalam menjaga stabilitas dan integritas sistem keuangan. Di Indonesia, pengawasan perbankan dilakukan oleh otoritas seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), yang bertugas memastikan bahwa bank mematuhi peraturan yang berlaku. OJK fokus pada pengawasan lembaga keuangan secara menyeluruh, termasuk penerapan prinsip tata kelola yang baik, perlindungan konsumen, dan kepatuhan terhadap regulasi seperti anti-pencucian uang serta pendanaan terorisme. Sementara itu, BI bertanggung jawab terhadap kebijakan moneter, sistem pembayaran, dan stabilitas sistem keuangan. Dalam penegakan aturan, sanksi administratif maupun hukum diterapkan terhadap bank yang melanggar ketentuan, baik berupa denda, pencabutan izin, maupun tindakan hukum lainnya. Selain itu, pengawasan berbasis risiko kini diterapkan untuk mengidentifikasi potensi masalah sebelum menjadi ancaman serius. Pendekatan ini mencerminkan upaya berkelanjutan otoritas dalam menciptakan sistem perbankan yang transparan, aman, dan stabil di tengah dinamika ekonomi global.

d. Perspektif Akademis dan Arah Masa Depan

Penelitian akademis memberikan wawasan berharga mengenai tantangan dan peluang dalam perlindungan data pribadi untuk perbankan seluler di Indonesia. Jurnal Universitas Jiaotong Barat Daya menyoroti perkembangan pesat teknologi informasi dan komunikasi

¹⁶ Maisah et al., "Analisis Hukum Terhadap Perlindungan Data Pribadi Nasabah Dalam Layanan Perbankan Digital Di Indonesia," *Aufklarung: Jurnal Pendidikan* 3, no. 3 (2023): 285–90.

¹⁷ Mahameru et al., "Implementasi Uu Perlindungan Data."

serta implikasinya terhadap perlindungan data pribadi di Indonesia. Penelitian ini menggarisbawahi perlunya adaptasi berkelanjutan terhadap kerangka regulasi untuk mengimbangi kemajuan teknologi. Prophetic Law Review menawarkan analisis tentang hak atas perlindungan data pribadi di Indonesia, menekankan pentingnya kerangka hukum yang kuat mengingat kemajuan teknologi terkini. Perspektif ini khususnya relevan dengan perbankan seluler, di mana persinggungan antara layanan keuangan dan teknologi digital menciptakan tantangan unik bagi perlindungan data. Awang Long Law Review membahas kurangnya regulasi hukum komprehensif di Indonesia terkait perlindungan data pribadi dan mengadvokasi undang-undang yang lebih kuat untuk melindungi data pribadi. Wacana akademis ini menyoroti kebutuhan berkelanjutan akan evolusi regulasi untuk mengatasi tantangan yang muncul di sektor perbankan seluler.¹⁸

Penerapan regulasi untuk melindungi data pribadi nasabah mobile banking di Indonesia merupakan lanskap yang kompleks dan terus berkembang. Kerangka regulasi yang komprehensif, yang mencakup UU PDP, UU ITE, dan regulasi sektoral, memberikan landasan yang kuat untuk perlindungan data. Namun, pesatnya kemajuan teknologi dalam mobile banking mengharuskan adaptasi dan penyempurnaan regulasi ini secara terus-menerus. Lembaga keuangan menanggapi tantangan ini dengan menerapkan solusi teknologi canggih dan praktik perlindungan data yang kuat. Meskipun demikian, tantangan yang berkelanjutan tetap ada, khususnya dalam menerapkan langkah-langkah perlindungan data yang komprehensif dalam lanskap perbankan digital yang berkembang pesat. Seiring dengan terus berkembangnya perbankan seluler di Indonesia, penerapan regulasi perlindungan data yang efektif akan menjadi sangat penting dalam menjaga kepercayaan konsumen dan memastikan keamanan informasi keuangan pribadi. Penelitian dan pengembangan regulasi di masa mendatang harus difokuskan pada penanganan teknologi yang baru muncul, ancaman siber yang terus berkembang, dan tantangan unik yang ditimbulkan oleh meningkatnya digitalisasi layanan perbankan.

SIMPULAN

Penelitian ini menyimpulkan bahwa mobile banking merupakan inovasi penting dalam perbankan digital yang memberikan kemudahan akses dan efisiensi transaksi bagi nasabah. Namun, layanan ini juga menghadirkan risiko terhadap keamanan data pribadi nasabah, seperti pencurian data dan eksploitasi ilegal. Regulasi di Indonesia, termasuk UU Perlindungan Data Pribadi (UU PDP) dan UU No. 10 Tahun 1998 tentang Perbankan, memberikan kerangka hukum untuk melindungi data nasabah, didukung oleh kebijakan OJK dan Bank Indonesia. Bank telah mengadopsi teknologi keamanan, seperti enkripsi SSL/TLS, biometrik, OTP, dan pengamanan berlapis untuk melindungi data nasabah. Namun, ancaman siber yang terus berkembang dan rendahnya literasi digital masyarakat menunjukkan perlunya penguatan perlindungan. Kolaborasi antara pemerintah, regulator, bank, dan masyarakat menjadi kunci untuk menciptakan ekosistem mobile banking yang aman dan terpercaya. Penelitian ini menekankan pentingnya peningkatan regulasi, pemanfaatan teknologi canggih, dan edukasi kepada nasabah untuk mengatasi tantangan tersebut.

Berdasarkan analisis perlindungan data pribadi nasabah terhadap penggunaan layanan mobile banking, terdapat beberapa saran yang dapat diimplementasikan untuk meningkatkan keamanan dan kepercayaan nasabah. Pemerintah dan regulator, seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), perlu terus memperbarui regulasi agar sejalan dengan perkembangan teknologi dan ancaman siber yang semakin kompleks. Regulasi, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), harus diterapkan secara efektif dengan sanksi yang tegas terhadap pelanggaran. Selain itu, bank perlu meningkatkan edukasi kepada nasabah mengenai pentingnya menjaga kerahasiaan data pribadi, seperti PIN dan OTP, melalui kampanye digital, seminar, atau pemberitahuan langsung dalam aplikasi mobile banking. Bank juga harus mengadopsi teknologi keamanan canggih, seperti enkripsi

¹⁸ Kiki Rezki Ramadhan and Chandra Wijaya2, "A New Decade for Social Changes," *Technium Social Sciences Journal* 6, no. December (2020): 101–5.

end-to-end, autentikasi biometrik, dan machine learning, untuk mencegah ancaman siber secara proaktif.

REFERENSI

- Akbar, Rohid, Muhammad Irwan, and Padli Nasution. "Journal of Sharia Economics Scholar (JoSES) Analisis Keamanan Data Pada Aplikasi Mobile Banking Journal of Sharia Economics Scholar (JoSES)" 2, no. 2 (2024): 79–83.
- Atsari, Amania Wahyu, Kristina Sulatri, and Muhammad Mashuri. "Perlindungan Hukum Bagi Nasabah Perbankan Terhadap Kesalahan Layanan Mobile Banking Dari Sistem Teknologi Informasi Perbankan." *Yurijaya : Jurnal Ilmiah Hukum* 5, no. 1 (2023): 59–72. <https://doi.org/10.51213/yurijaya.v5i1.97>.
- Budiarto, Agung, and Pujiyono. "Perlindungan Hukum Nasabah Pengguna Mobile Banking." *Jurnal Privat Law* 9, no. Vol 9, No 2 (2021): JULI-DESEMBER (2021): 300–308.
- Hanafitty. "ANALISIS PERLINDUNGAN KERAHASIAAN DATA PRIBADI PADA NASABAH PENGGUNA PRODUK LAYANAN MOBILE BANKING BANK MILIK THE ANALYSIS OF THE SECURITY PROTECTION OF PRIVACY DATA ON THE CUSTOMER OF MOBILE BANKING SERVICE PRODUCT IN ACEH PROVINCIAL PENDAHULUAN Bank Mil." *Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan* 5, no. 2 (2021): 328–37.
- Irmawati, Ema, John Pieries, and Wiwik Sri Widiarty. "PERLINDUNGAN HUKUM ATAS DATA PRIBADI NASABAH BANK PENGGUNA MOBILE BANKING DALAM PERSPEKTIF UU NO 27 TAHUN 2022 TENTANG KEBOCORAN DATA." *Syntax Admiration* 15, no. 1 (2024): 37–48.
- Kajian, Jurnal, Hukum Dan, Pendidikan Kewarganegaraan, Sidik Sunaryo, and Jatmiko Wahyu Utomo. "Perlindungan Hukum Preventif Oleh Ojk Dalam Mencegah Kebocoran Data Pribadi Konsumen Pinjaman Online Berdasarkan Peraturan Ojk Nomor 06/Pojk.07/2022 Tentang Perlindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan." *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan* 3 (2023): 1–9.
- Mahameru, Danil Erlangga, Aisyah Nurhalizah, Ahmad Wildan, Mochamad Haikal, and Mohamad Haikal Rahmadia. "Implementasi Uu Perlindungan Data" 5, no. 20 (2023): 115–31.
- Maisah, Sinta Pala Sari, Sudiarni, and Himsar Pariaman Ompusunggu. "Analisis Hukum Terhadap Perlindungan Data Pribadi Nasabah Dalam Layanan Perbankan Digital Di Indonesia." *Aufklarung: Jurnal Pendidikan* 3, no. 3 (2023): 285–90.
- Rahmahdhani, Dinda Novika, Muhammad Irwan Padli Nasution, and Sri Suci Ayu Sundari. "Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking." *JUEB : Jurnal Ekonomi Dan Bisnis* 2, no. 2 (2023): 88–96. <https://doi.org/10.57218/jueb.v2i2.693>.
- Ramadhan, Kiki Rezki, and Chandra Wijaya2. "A New Decade for Social Changes." *Technium Social Sciences Journal* 6, no. December (2020): 101–5.
- Sihotang, Lidia, and Ilham Hudi. "Penerapan M-Banking Dalam Meningkatkan Jasa, Layanan Perbankan Di Bank Rakyat Indonesia Kantor Cabang Pekanbaru Sudirman." *Jurnal Akuntansi AKTIVA* 4, no. 2 (2023): 106–14. <https://doi.org/10.24127/akuntansi.v4i2.4831>.
- Tarigan, Herdian Ayu Andreana Beru, and Darminto Hartono Paulus. "Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital." *Jurnal Pembangunan Hukum Indonesia* 1, no. 3 (2019): 294–307. <https://doi.org/10.14710/jphi.v1i3.294-307>.
- DBS, digibank by. 2021. *Ini Tips Agar Mobile Banking Anda Tetap Aman*. 25 Mei. Accessed Mei 25, 2021. <https://www.dbs.id/digibank/id/id/articles/tak-mau-kena-bobol-ini-tips-agar-mobile-banking-anda-tetap-aman?form=MG0AV3>.