Jurnal Hukum Progresif

Vol 7 No 11, November 2024
EISSN : 24490120

PERLINDUNGAN HUKUM BAGI NASABAH PENGGUNA MOBILE BANKING DALAM MENGHADAPI RISIKO CYBERCRIME DAN KEBOCORAN DATA PRIBADI

Laila Nur Aulia Putri[1], Nabila Salma Taqwa[2]
lailanputri@students.unnes.ac.id[1], nabilasalmat@students.unnes.ac.id[2]
Universitas Negeri Semarang

Abstrak: Perkembangan teknologi informasi, khususnya dalam sektor perbankan melalui layanan mobile banking, membawa dampak positif terhadap kemudahan transaksi keuangan. Namun, seiring dengan kemajuan teknologi tersebut, muncul ancaman baru berupa kejahatan dunia maya (cybercrime) yang menargetkan nasabah serta data pribadi mereka. Perlindungan hukum terhadap nasabah pengguna mobile banking menjadi sangat penting untuk menjaga privasi dan keamanan data mereka. Artikel ini mengkaji perlindungan hukum bagi pengguna mobile banking di Indonesia dengan menggunakan metode yuridis normatif, yakni dengan menganalisis peraturan perundang-undangan yang memberikan perlindungan bagi nasabah dari ancaman cybercrime. Fokus kajian ini meliputi Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, dan Undang-Undang Informasi dan Transaksi Elektronik (ITE). Selain itu, artikel ini juga mengulas tanggung jawab bank dalam melindungi nasabah dari ancaman kejahatan siber serta upaya hukum yang dapat ditempuh oleh nasabah yang menjadi korban. Penelitian ini menemukan bahwa meskipun terdapat dasar hukum yang cukup kuat untuk melindungi nasabah, penerapan regulasi yang lebih ketat dan peningkatan kesadaran dari pihak bank maupun nasabah sangat diperlukan untuk mengurangi risiko kerugian akibat kejahatan dunia maya.
Kata Kunci: Mobile Banking, Cybercrime, Perlindungan Hukum, Perbankan, Data Pribadi.

Abstract: *The development of information technology, particularly in the banking sector through mobile banking services, has a positive impact on the ease of financial transactions. However, along with technological advancements, new threats have emerged in the form of cybercrimes targeting customers and their personal data. Legal protection for mobile banking users is crucial to safeguard their privacy and data security. This article examines the legal protection for mobile banking users in Indonesia using a normative juridical approach, analyzing the regulations that provide protection for customers against cybercrime threats. The focus of this study includes the Banking Law, the Consumer Protection Law, and the Electronic Information and Transactions Law (ITE Law). Additionally, this article discusses the responsibility of banks in protecting customers from cyber threats and the legal recourse available to customers who become victims. This research finds that although there is a strong legal foundation to protect customers, stricter regulation enforcement and increased awareness from both banks and customers are needed to reduce the risk of losses due to cybercrimes.*
Keywords: *Mobile Banking, Cybercrime, Legal Protection, Banking, Personal Data.*

PENDAHULUAN

Dalam era globalisasi, teknologi semakin maju sebagai sarana pendukung dalam aktivitas sehari-hari manusia. Dunia digital pada masa kini sudah tida dapat dipisahkan dari kehidupan masyarakat, seolah menjadi kebutuhan dasar. Di masa kini, kehidupan sangat berpengaruh oleh teknologi, khususnya dunia maya. Seiring perkembangan zaman, terutama dengan hadirnya internet, banyak inovasi bermunculan di bermacam-macam aspek kehidupan, termasuk dunia bisnis. Kini, orang memandang internet sebagai sarana untuk melaksanakan aktivitas dan memenuhi kebutuhan orang-orang dengan cara yang lebih cepat dan optimal. Kemajuan teknologi pada masa kini mendorong beberapa pihak untuk bersiap bersaing dalam menghasilkan inovasi yang menarik minat masyarakat. Salah satu terobosan yang dihasilkan adalah di bidang perbankan. Dahulu, untuk mengambil uang, melakukan transfer, atau untuk transaksi lain, kita perlu mengunjungi bank dan sering kali perlu menunggu dalam antrian panjang, dari pagi hingga siang. Dengan berkembangnya kemajuan zaman, muncul inovasi di sektor perbankan menghadirkan layanan e-banking atau perbankan elektronik yang berbasis internet. (Yuslia, 2018).

Digital banking mencakup berbagai layanan perbankan yang bisa dibuka menggunakan perangkat elektronik seperti komputer, smartphone, atau tablet. Era ekonomi digital ditandai dengan integrasi teknologi informasi dan komunikasi ke dalam berbagai aspek aktivitas ekonomi. Digital banking merupakan jasa perbankan yang memfasilitasi pelanggan yang sedang melakukan transaksi finansial melewati internet maupun aplikasi mobile banking. Perkembangan era ekonomi digital telah mempermudah akses terhadap layanan perbankan ini (). Internet banking menawarkan banyak sekali manfaat, baik bagi nasabah maupun bagi pihak bank. Namun, dibalik selain berbagai manfaat yang ditawarkan, layanan ini juga berpotensi menimbulkan dampak negatif. Salah satu konsekuensi negatif penggunaan internet banking adalah munculnya risiko kejahatan di bidang perbankan, seperti pencurian data nasabah dan nomor kartu kredit, dimana data atau nomor yang dicuri tersebut kemudian disalahgunakan oleh pihak yang tidak berwenang (Benedictus, 2022).

Digital banking semakin populer karena kenyamanan dan efisiensi waktu yang ditawarkannya. Perlindungan nasabah dalam penggunaan layanan digital banking menjadi isu penting, mengingat adanya ancaman keamanan seperti pencurian identitas, penipuan, gangguan transaksi, serangan malware yang dapat mengganggu sistem keamanan digital banking, serta risiko kebocoran data pribadi (Dewi, Widya & Faricha, 2023). Seiring dengan kemajuan teknologi informasi, semakin banyak pihak ketiga yang melakukan kejahatan siber dengan memanfaatkan celah keamanan di dunia digital. Peretas kini mampu mengeksploitasi sistem, yang berpotensi mengancam keamanan layanan perbankan digital nasional. Serangan dari pihak tak bertanggung jawab ini dapat menyebabkan kerusakan signifikan pada sistem keamanan perbankan, membuka peluang terjadinya pencurian data, peretasan akun, hingga gangguan dalam transaksi keuangan. Kejahatan siber ini menyoroti pentingnya perlindungan yang lebih ketat terhadap sistem perbankan digital dan keamanan nasabah (Zulina, 2024).

Cybercrime adalah jenis kejahatan yang dapat terjadi tanpa batas wilayah dan tanpa memerlukan antar hubungan pelaku dan korban. Berhubungan dengan pengertian tersebut, berbagai negara, termasuk Indonesia, pihak terlibat dalam aktivitas internet akan merasakan dampak dari berkembangnya kejahatan dunia maya (Benedictus, 2022). Lebih jauh lagi, pelaku kejahatan kini memanfaatkan kecanggihan teknologi informasi dan komputer untuk tujuan pencucian uang dan aksi terorisme. Oleh karena itu, dengan meningkatnya kejahatan, khususnya yang melibatkan layanan internet banking, industri perbankan perlu menyiapkan fitur keamanan yang dapat menjaga keyakinan nasabah sesungguhnya transaksi elektronik terpercaya. Indonesia diakui salah satu negara dengan resiko tinggi terhadap serangan IT.

Dalam sektor perbankan, jenis kejahatan yang sering terjadi adalah man in the middle attack dan trojan horses, yang dapat mengancam keamanan layanan. Man in the middle attack melibatkan

pelaku yang menciptakan situs web tiruan mirip dengan situs bank untuk mengelabui nasabah dan mencuri data. Sementara itu, trojan horses adalah program berbahaya yang disisipkan ke aplikasi umum di komputer pengguna. Saat pengguna login ke situs banknya, penyerang dapat mengambil alih sesi untuk melakukan transaksi tanpa terdeteksi.

Saat ini, ada banyak undang-undang yang melindungi transaksi online dari data pribadi, seperti Undang-Undang Perlindungan Data Pribadi atau undang-undang lain yang mengatur privasi informasi pribadi. Selain itu, kebijakan privasi yang diterapkan oleh situs web, seperti kebijakan privasi, pengumuman privasi, dan ketentuan layanan, juga membantu melindungi data pribadi. Menurut Yuslia (2018), tujuan utama dari peraturan perlindungan data pribadi adalah untuk memberikan hak kepada individu untuk mengendalikan dan mengakses informasi pribadi yang dikumpulkan oleh pihak lain. Peraturan juga memberikan hak kepada individu untuk melakukan perbaikan terhadap data tersebut jika diperlukan.

Cybercrime adalah isu yang sangat serius dan tidak boleh dipandang sebelah mata. Dampaknya dapat merugikan, baik secara finansial bagi nasabah maupun dalam hal hilangnya kepercayaan nasabah terhadap lembaga keuangan. Korban dari cybercrime bisa kehilangan uang mereka, sementara bank sebagai lembaga keuangan juga berisiko mengalami kerusakan reputasi yang besar. Oleh karena itu, perlindungan nasabah dari ancaman cybercrime harus menjadi prioritas utama bagi bank (Akhmad & Basuki, 2024).

Pihak perbankan perlu lebih aktif memberikan informasi kepada masyarakat, nasabah, dan pegawai mengenai berbagai bentuk kejahatan yang dapat terjadi melalui produk atau layanan yang mereka sediakan. Meskipun teknologi dan peraturan hukum saat ini telah meningkatkan keamanan internet banking, perbankan dan pemerintah harus terus berupaya untuk memastikan bahwa penyelenggaraan internet banking tetap terjaga keamanannya. Namun, masih ada anggapan bahwa pelaku usaha perbankan dan masyarakat pada umumnya kurang peduli atau belum cukup sadar terhadap penanganan kasus tindak pidana yang terkait dengan internet banking, diperlukan langkah-langkah menyeluruh dari semua pihak untuk memperbaiki situasi ini.

Dengan demikian, Berdasarkan penjelasan yang telah disampaikan sebelumnya, tulisan ini merumuskan dua permasalahan utama, yaitu: (1) Perlindungan Hukum bagi Nasabah Pengguna Mobile Banking Terhadap Cybercrime, (2) Tanggung Jawab oleh Pihak Bank Akibat Cybercrime.

METODE PENELITIAN

Penelitian ini mengaplikasikan metode penelitian. yuridis normatif yang bertujuan memberikan jawaban atas masalah hukum melalui pendekatan yuridis, terutama dalam situasi kekosongan hukum, ketidakjelasan, atau konflik antara peraturan perundang-undangan. Metode ini fokus pada analisis terhadap norma-norma hukum yang berlaku untuk memberikan solusi atas permasalahan hukum yang menjadi objek penelitian ini meliputi sumber data berupa bahan hukum primer, seperti undang-undang dan peraturan perundang-undangan, seperti peraturan perundang-undangan, putusan pengadilan, dan dokumen resmi lainnya yang relevan dengan topik penelitian, serta bahan hukum sekunder, seperti buku, jurnal ilmiah, dan literatur terkait yang mendukung analisis terhadap bahan primer. Data dikumpulkan melalui studi pustaka dengan menggunakan pendekatan peraturan perundang-undangan, di mana peraturan-peraturan yang relevan dianalisis dan diinterpretasikan untuk memahami implikasinya terhadap isu yang dibahas. Dengan menggunakan metode ini, peneliti dapat merumuskan solusi hukum yang komprehensif berdasarkan analisis normatif yang mendalam, sehingga memberikan kontribusi pada pengembangan ilmu hukum.

HASIL DAN PEMBAHASAN

A. Perlindungan Hukum bagi Pengguna Mobile Banking dari Kejahatan Siber dan Kebocoran Data Pribadi Berdasarkan Peraturan Perundang-Undangan yang Berlaku di Indonesia

Perkembangan pesat teknologi informasi telah memberikan dampak signifikan pada berbagai sektor, termasuk industri perbankan. Salah satu inovasi yang penting dalam sektor ini adalah layanan Internet Banking, yang memudahkan nasabah untuk melakukan berbagai transaksi perbankan, seperti membuka rekening, mentransfer uang, dan membayar tagihan secara online melalui internet. Dalam mengelola layanan perbankan elektronik (e-banking), bank diwajibkan untuk menerapkan manajemen risiko yang baik guna menjaga keamanan dan kenyamanan nasabah. Hal ini sangat krusial mengingat layanan e-banking memiliki potensi risiko tinggi, seperti ancaman peretasan yang bisa menembus sistem keamanan, termasuk firewall, atau melalui situs palsu yang meniru domain resmi. (Astrini, D. A., 2015).

Hingga saat ini, di Indonesia belum ada undang-undang yang secara khusus mengatur layanan internet banking. Meskipun demikian, terdapat berbagai peraturan yang dapat dijadikan acuan hukum untuk melindungi pengguna layanan tersebut. Dalam implementasinya, bank biasanya merujuk pada sejumlah regulasi yang relevan guna memastikan perlindungan hukum bagi nasabah yang menggunakan layanan internet banking.

Undang-undang Nomor 7 Tahun 1992 yang diubah menjadi Undang-undang Nomor 10 Tahun 1998 tentang Perbankan

Undang-Undang Nomor 7 Tahun 1992 yang kemudian diubah menjadi Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan memberikan perhatian khusus terhadap privasi dan keamanan data nasabah, termasuk dalam penggunaan Internet Banking. Layanan ini memiliki potensi rentan terhadap pelanggaran perlindungan data pribadi pengguna. Berdasarkan Pasal 29 ayat (4) UU Nomor 10 Tahun 1998, bank diwajibkan memberikan informasi mengenai risiko kerugian yang mungkin timbul akibat transaksi yang dilakukan. Ketentuan ini sangat penting dalam layanan Internet Banking, di mana bank perlu memberikan edukasi kepada nasabah mengenai potensi risiko yang ada. Namun, prinsip kerahasiaan dalam undang-undang ini hanya mencakup data yang disimpan atau dikumpulkan oleh bank, sementara pada layanan Internet Banking, data nasabah juga meliputi informasi yang dikirim melalui perangkat mereka. Ini menunjukkan pentingnya penguatan perlindungan data nasabah dalam layanan berbasis digital. (Nugraheni, T. dkk., 2024).

Perlindungan data pribadi nasabah diatur secara tegas dalam Pasal 40 ayat (1) UU Perbankan, yang mengharuskan bank untuk menjaga kerahasiaan informasi nasabah, kecuali dalam kondisi tertentu yang diatur dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44, dan Pasal 44A. Prinsip kerahasiaan ini melarang bank untuk mengungkapkan atau membagikan data nasabah tanpa alasan yang sah. Jika terjadi pelanggaran, Pasal 47 ayat (2) UU Perbankan menetapkan hukuman berupa penjara minimal dua tahun dan denda antara Rp4 miliar hingga Rp8 miliar bagi pihak yang dengan sengaja membocorkan informasi yang harus dijaga kerahasiaannya. (Widayanti, W. P., 2022).

Undang-undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen

Sebagaimana diatur dalam Pasal 1 angka 1 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK), tujuan perlindungan konsumen adalah untuk memberikan jaminan kepada konsumen. Serangkaian tindakan yang diambil untuk memastikan hak-hak konsumen dilindungi secara hukum dikenal sebagai perlindungan konsumen. Untuk mencegah konsumen berada dalam posisi yang tidak menguntungkan, tujuan utama perlindungan ini adalah menciptakan keseimbangan antara pelaku usaha dan konsumen.

Pasal 28D ayat (1) UU 1945 menetapkan dasar perlindungan Indonesia, menyatakan bahwa "Setiap orang berhak memperoleh pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang setara di hadapan hukum." Menurut ketentuan ini, setiap orang berhak atas perlindungan hukum, termasuk keselamatan saat menggunakan barang atau jasa.

Pasal 26 UUPK mengatur bahwa pelaku usaha yang memperdagangkan jasa wajib memberikan jaminan atau garansi sesuai dengan kesepakatan atau perjanjian yang berlaku. Sebagai contoh, bank yang menyediakan layanan internet banking sering mempromosikan keamanan sebagai salah satu keunggulan layanannya. Namun, dalam praktiknya, sistem keamanan tersebut masih dapat ditembus, menunjukkan bahwa kewajiban bank dalam memberikan perlindungan keamanan belum sepenuhnya terpenuhi. Hal ini menunjukkan adanya celah dalam penerapan hukum, di mana belum tersedia mekanisme yang tegas untuk menindak pelanggaran atau kegagalan memenuhi kewajiban tersebut.

Selain itu, UUPK juga mengatur pemberlakuan sanksi hukum sebagai bentuk perlindungan represif, yang bertujuan memberikan efek jera bagi pelaku usaha yang melanggar ketentuan. Dalam Pasal 60 hingga Pasal 63 UUPK, tercantum berbagai jenis sanksi yang dapat dikenakan, mulai dari sanksi administratif hingga sanksi pidana. Sanksi administratif dapat berupa peringatan tertulis, pengumuman publik tentang pelanggaran yang dilakukan, atau pemberian denda administratif. Sementara itu, sanksi pidana, meskipun hanya diterapkan pada pasal tertentu, dirancang untuk memberikan hukuman yang lebih tegas. Di sisi lain, sanksi perdata dalam bentuk ganti rugi dapat diberikan kepada konsumen yang mengalami kerugian akibat tindakan pelaku usaha. Pemberlakuan sanksi ini bertujuan untuk memastikan bahwa pelaku usaha bertanggung jawab atas perbuatannya sekaligus mencegah terjadinya kerugian serupa di masa mendatang. (Astrini, D. A., 2015).

Undang-Undang Nomor 19 Tahun 2016 yang merupakan amandemen dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Untuk melindungi orang-orang yang menggunakan teknologi informasi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur berbagai hal penting, seperti mengakui informasi dan dokumen elektronik sebagai alat bukti yang sah secara hukum, mengakui tanda tangan elektronik, dan mengatur sertifikasi dan sistem elektronik. Selain itu, UU ITE menekankan betapa pentingnya menjalankan sistem elektronik yang aman dan dapat diandalkan, terutama untuk penyedia layanan seperti institusi perbankan.

Dalam UU ITE, pemerintah mewajibkan setiap penyelenggara sistem elektronik untuk memastikan sistem yang mereka kelola berfungsi dengan lancar, aman, dan dapat dipercaya. Pasal 15 ayat (1) mengatur bahwa penyelenggara sistem elektronik, termasuk bank, harus memastikan pengelolaan sistem yang handal dan aman serta bertanggung jawab atas operasionalnya. Pasal 15 ayat (2) menegaskan bahwa penyelenggara sistem elektronik memiliki tanggung jawab penuh terhadap kelancaran operasional sistem tersebut. Namun, Pasal 15 ayat (3) memberikan pengecualian, di mana tanggung jawab ini tidak berlaku jika penyelenggara dapat membuktikan adanya keadaan darurat, kesalahan, atau kelalaian dari pihak pengguna yang menyebabkan gangguan atau kerugian.

Berdasarkan ketentuan dalam Pasal 15 ayat (1), (2), dan (3), bank sebagai penyelenggara sistem elektronik memiliki kewajiban untuk menanggung kerugian yang dialami nasabah akibat kegagalan sistem yang tidak berfungsi dengan baik. Namun, jika bank dapat membuktikan bahwa kerugian tersebut disebabkan oleh kesalahan atau kelalaian nasabah, maka bank dapat dibebaskan dari tanggung jawab. Oleh karena itu, peraturan ini tidak hanya memberikan perlindungan bagi nasabah, tetapi juga menegaskan pentingnya tanggung jawab bersama antara penyelenggara dan pengguna sistem elektronik untuk memastikan keamanan dan kelancaran transaksi (Rennysee, B., 2022).

Dalam kasus pencurian data pribadi nasabah, data pribadi menjadi elemen yang sangat penting dan sering menjadi sasaran tindakan kriminal. Di Indonesia, meskipun belum ada regulasi yang secara eksplisit mengatur perlindungan data pribadi, hal ini diatur secara tidak langsung melalui Undang-Undang Nomor 19 Tahun 2016 yang merupakan perubahan dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini mencakup berbagai aspek mengenai informasi elektronik dan transaksi digital serta memberikan perlindungan terhadap privasi pengguna, termasuk nasabah yang memanfaatkan layanan perbankan berbasis

elektronik.

Dalam hal pencurian data pribadi, UU ITE menetapkan ketentuan yang tegas mengenai sanksi terhadap pelaku kejahatan yang melibatkan data pribadi nasabah. Beberapa pasal yang relevan termasuk Pasal 30, Pasal 32, dan Pasal 35, yang mengatur tindak pidana terkait dengan akses ilegal ke sistem elektronik untuk mencuri data atau informasi. Selain itu, ketentuan pidana lebih lanjut dapat ditemukan dalam Pasal 46, Pasal 48, Pasal 49, dan Pasal 51, yang memberikan dasar hukum untuk proses penuntutan dan pemberian sanksi kepada pelaku yang melanggar ketentuan mengenai perlindungan. Pasal 46 dan Pasal 30 UU ITE menetapkan sanksi bagi pelaku pencurian data pribadi, khususnya mereka yang mengakses sistem elektronik dengan cara yang melanggar pengamanan yang ada, yang dapat dikenakan hukuman penjara selama 6 hingga 8 tahun dan/atau denda yang sangat besar, yaitu antara Rp600.000.000 dan Rp800.000.000. Hal ini menunjukkan betapa pentingnya perlindungan data pribadi di Indonesia karena potensi kerugian yang signifikan jika data pelanggan dicuri atau disalahgunakan oleh individu yang tidak bertanggung jawab (Widayanti, W. P., 2022).

Peraturan Bank Indonesia Nomor 7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah

Peraturan Bank Indonesia Nomor 7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah, Pasal 1, angka 6, mendefinisikan data pribadi nasabah sebagai informasi yang berkaitan dengan identitas nasabah yang biasanya diberikan kepada bank untuk tujuan transaksi keuangan. Oleh karena itu, data pribadi sangat penting untuk banyak layanan perbankan, seperti membuat kartu kredit, kartu debit, dan lainnya. Data ini berfungsi sebagai dasar untuk berbagai kegiatan yang berkaitan dengan keuangan.

Indonesia, sebagai negara dengan tingkat penggunaan teknologi dan informasi yang tinggi, memanfaatkan teknologi ini di berbagai sektor, termasuk pemerintahan, perbankan, keuangan, hingga pendidikan. Pesatnya perkembangan teknologi telah mengubah pola kehidupan masyarakat, memberikan kemudahan dalam berbagai aspek kehidupan sehari-hari.

Namun, dibalik manfaat yang ditawarkan, penggunaan teknologi juga menghadirkan tantangan baru, khususnya terkait perlindungan hukum atas data pribadi. Teknologi tidak hanya mempermudah proses transaksi, tetapi juga membuka celah bagi permasalahan hukum, salah satunya adalah isu perlindungan data pribadi (the protection of privacy rights) dalam layanan perbankan. Pasal 1 angka 3 Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia menggambarkan perlindungan konsumen sebagai kepastian hukum yang menjamin hak-hak konsumen. Oleh karena itu, tujuan utama dari perlindungan ini adalah untuk melindungi hak-hak konsumen, termasuk menjaga keamanan data pribadi mereka selama setiap transaksi yang mereka lakukan (Maulana, A. R., dan Apriani, R., 2021).

B. Tanggung Jawab oleh Pihak Bank Akibat Cybercrime

Kejahatan yang terjadi di sektor perbankan melibatkan berbagai tindak pidana yang berhubungan langsung dengan aktivitas perbankan, seperti perampokan bank atau pemindahan dana secara ilegal, yang mana definisinya cukup luas. Sementara itu, tindak pidana perbankan merujuk pada pelanggaran yang diatur dalam peraturan perundang-undangan perbankan, yang mencakup larangan-larangan dan kewajiban-kewajiban, seperti pelarangan pendirian bank ilegal dan kewajiban menjaga kerahasiaan informasi bank. Di sisi lain, cybercrime merupakan jenis kejahatan baru yang semakin mendapatkan perhatian global. Dalam pengertian sempit, cybercrime mencakup kejahatan yang secara langsung menargetkan sistem komputer atau jaringan. Namun, secara lebih luas, cybercrime juga meliputi berbagai kejahatan baru yang menargetkan komputer, jaringan, serta penggunaannya, termasuk kejahatan konvensional yang kini dilakukan dengan bantuan teknologi komputer (Nunuk, 2018).

Informasi mengenai nasabah dan keuangannya wajib dijaga kerahasiaannya dan tidak boleh diungkapkan oleh pihak manapun atau untuk alasan apapun. Bank bertanggung jawab penuh atas

pelanggaran yang mungkin terjadi terkait kerahasiaan data nasabah. Dalam hal ini, bank memiliki kewajiban hukum untuk melindungi data tersebut dari akses atau penggunaan yang tidak sah. Namun, berdasarkan teori relatif, kerahasiaan informasi tentang nasabah dan keuangannya yang tersimpan di bank tetap harus dipatuhi, kecuali dalam situasi tertentu yang diperbolehkan oleh Undang-Undang. Dalam kondisi demikian, bank diizinkan untuk membuka data tersebut kepada pihak berwenang yang memiliki alasan sah dan dasar hukum yang kuat untuk memintanya (Yuslia, 2018).

Hubungan antara bank dan nasabah merupakan suatu kegiatan yang melibatkan tanggung jawab penuh, yang diatur oleh ketentuan dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Pihak bank memberikan perlindungan kepada nasabah melalui dua metode, yaitu perlindungan tersirat dan perlindungan yang eksplisit. dilakukan dengan merujuk pada undang-undang perbankan yang menjadi dasar aturan yang diterapkan. Sementara perlindungan eksplisit dilakukan dengan melibatkan lembaga masyarakat untuk menjamin dana nasabah jika terjadi kejadian yang tidak diinginkan.

Permasalahan di sektor perbankan, terutama yang berkaitan dengan cybercrime, semakin marak terjadi. Bank perlu bertanggung jawab agar nasabah mendapatkan perlindungan dan pemulihan dari kejahatan peretasan tersebut. Penjualan data nasabah juga mempengaruhi perekonomian negara, karena berpotensi menurunkan kepercayaan masyarakat terhadap bank nasional. Oleh karena itu, diperlukan adanya tanggung jawab hukum atas masalah ini. Tanggung jawab hukum melibatkan kewajiban untuk memenuhi kewenangan dan tanggung jawab yang muncul yakni tindakan yang dilaksanakan. Terdapat beberapa bentuk tanggung jawab hukum yang termuat dalam undang-undang. Asas pertanggungjawaban merupakan prinsip mengatur tanggung jawab dalam pemrosesan dan pengawasan data pribadi, dengan memastikan tindakan yang dilakukan secara bertanggung jawab. Asas ini bertujuan untuk memastikan bola antara hak dan kewajiban semua pihak yang terlibat, termasuk pemilik data pribadi (Irma, Nova, Diyah & Sandro, 2023).

Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) menyebutkan bahwa "Setiap perbuatan melanggar hukum yang menyebabkan kerugian bagi orang lain mewajibkan pelaku, karena kesalahannya, untuk mengganti kerugian tersebut." Dalam peraturan yang mengatur sektor jasa keuangan, bank memiliki kewajiban untuk bertanggung jawab atas kerugian yang dialami oleh nasabahnya. Ketentuan ini juga diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. (Subaidah, Dhian, & Dian, 2023). Pasal 3 UU ITE menetapkan bahwa prinsip kehati-hatian harus diterapkan, dan mewajibkan setiap penyelenggara sistem elektronik (PSE), baik dari sektor perusahaan ataupun instansi, guna menjalankan tanggung jawab dalam penyelenggaraan sistem elektronik yang dapat diandalkan, aman, dan bertanggung jawab. Sebagai penyedia layanan transaksi elektronik melalui mobile banking, pihak bank seharusnya memikul tanggung jawab penuh, mengingat tingginya risiko dan berbagai macam potensi masalah yang terkait dengan transaksi menggunakan sistem mobile banking. Oleh karena itu, bank perlu menerapkan prinsip kehati-hatian secara lebih ketat dalam pengelolaan dan penggunaan sistem mobile banking oleh nasabahnya (Made, 2020).

Sebelum menentukan bentuk pertanggungjawaban yang akan dilakukan oleh pihak sebelum itu, penting untuk terlebih dahulu menetapkan kedudukan hukum atau legal standing korban, yang menurut ketentuan hukum adalah pihak yang memiliki hubungan hukum yang sah dengan pihak perbankan. Pembuktian atas hal ini akan merujuk pada relasi antara kedua belah pihak sesuai dengan ketentuan hukum yang berlaku. atau perjanjian yang telah disepakati oleh keduanya. Pertama, berdasarkan Pasal 1320 KUHPerdata, terdapat kegagalan dalam memenuhi asas perikatan yang menjadi bagian dari operasional perbankan. yang pada dasarnya memberikan kewenangan kepada pihak Bank untuk melaksanakan kegiatan usahanya terkait dengan dana simpanan nasabah. Kedua, berdasarkan Pasal 4 Ayat (1) UU Perlindungan Konsumen, hak nasabah sebagai konsumen yang

menggunakan jasa perbankan untuk menyimpan dana atau uang miliknya tidak terpenuhi.

Apabila nasabah sebagai penyimpan dana dapat membuktikan kedua hal tersebut, maka posisi hukum nasabah sebagai korban akan semakin kokoh. Hal ini memberikan dasar yang kuat bagi nasabah untuk mengajukan klaim ganti rugi atas kerugian yang disebabkan oleh kelalaian atau tindakan sengaja dari pihak perbankan. Klaim tersebut dijamin oleh peraturan perundang-undangan yang mengatur hak-hak nasabah serta kewajiban bank menjalankan operasionalnya. Dengan bukti yang kuat, nasabah dapat mengajukan klaim untuk memperoleh kompensasi yang sesuai, sebagai bentuk perlindungan hukum atas kerugian yang dialami (Muhammad. Muhammad & Revy, 2024).

Pasal 19 ayat (1) Undang-Undang Perlindungan Konsumen mengatur bahwa pelaku usaha, termasuk perbankan, wajib memberikan ganti rugi atas kerugian yang dialami konsumen akibat penggunaan jasa yang disediakannya. Perlindungan hukum bagi nasabah bank yang menderita kerugian akibat kejahatan skimming juga diatur dalam Peraturan Bank Indonesia Nomor 16/1/PBI/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran. Pasal 10 peraturan ini menyatakan, "Penyelenggara bertanggung jawab kepada konsumen atas kerugian yang terjadi akibat kesalahan pengurus dan pegawai penyelenggara." Perlindungan konsumen jasa sistem pembayaran, yang dikenal sebagai perlindungan konsumen, mencakup segala upaya untuk menjamin adanya kepastian hukum guna melindungi konsumen layanan sistem pembayaran atau yang disebut perlindungan konsumen, adalah segala upaya untuk memastikan adanya kepastian hukum guna melindungi konsumen layanan sistem pembayaran (Subaidah, Dhian, & Dian, 2023).

Bank memiliki kewajiban untuk mengganti kerugian nasabah yang menjadi korban cybercrime, apabila terbukti bank lalai dalam menjalankan kewajibannya, termasuk dalam menjaga keamanan dan ketahanan sistem elektronik yang dimilikinya. Jika kewajiban ini tidak dipenuhi, bank dapat dikenakan sanksi administratif, seperti peringatan tertulis atau denda. Konsumen yang mendaptkan kerugian materiil dari dampak bank dapat mengajukan pengaduan sesuai dengan mekanisme yang diatur oleh peraturan yang berlaku. Bentuk pertanggungjawaban bank atas penggunaan internet banking akan bergantung pada penyebab kerugian tersebut, dan apabila kerugian materiil disebabkan oleh kelalaian pihak bank, maka bank wajib memberikan ganti rugi sesuai tuntutan nasabah. Namun, nasabah tetap harus memenuhi persyaratan yang diminta oleh bank agar proses pengecekan terhadap transaksi mobile banking yang gagal dapat dilakukan dengan mudah (Made, 2020).

Dalam hal pertanggungjawaban, bank mengadopsi prosedur penyelesaian yang dimulai dengan menerima laporan dari nasabah yang menjadi korban tindak pidana cybercrime, baik melalui call center yang tersedia maupun secara tertulis. Laporan ini kemudian diproses sesuai prosedur yang ada, dengan memberikan bantuan dan solusi kepada nasabah yang terdampak. Untuk memastikan perlindungan hukum bagi nasabah pengguna layanan internet banking, bank mengikuti ketentuan dalam Surat Keputusan Nomor 055 Tahun 2023 mengenai Pedoman Layanan Pengaduan Nasabah dan Perlindungan Konsumen. Surat keputusan ini mengatur berbagai prinsip perlindungan yang harus diterapkan oleh bank, termasuk kewajiban untuk melaporkan gangguan yang signifikan kepada Bank Indonesia, dengan menyertakan informasi terkait penyebab, dampak, dan langkah-langkah penyelesaian yang diambil. Ketentuan ini memberikan kesempatan bagi regulator untuk memantau situasi dan memberikan arahan jika diperlukan.

Untuk melindungi hak-hak hukum pengguna layanan internet banking, bank akan mengambil langkah-langkah proaktif dengan melaporkan kasus kejahatan siber dan mendampingi korban untuk melaporkan kejadian tersebut ke pihak kepolisian agar dapat diproses sesuai hukum yang berlaku. Bank bertanggung jawab terhadap nasabah yang menjadi korban kejahatan siber sesuai dengan ketentuan pengajuan klaim. Apabila kerugian disebabkan oleh kelalaian nasabah, maka nasabah tidak berhak mengajukan klaim kepada bank, meskipun bank tetap akan membantu mencari solusi atas permasalahan tersebut. Namun, jika kerugian timbul akibat kelalaian bank sebagai penyedia layanan internet banking, bank wajib memenuhi klaim nasabah dan memberikan kompensasi yang sesuai.

Sebaliknya, jika kerugian diakibatkan oleh tindakan pihak ketiga, maka tanggung jawab untuk memenuhi tuntutan ada pada pihak ketiga tersebut nasabah (Tri, Aksi & Darius, 2024).

Melihat permasalahan yang muncul terkait dengan kepastian hukum dalam transaksi mobile banking, terutama yang berkaitan dengan aspek keamanan transaksi dan tanggung jawab bank jika nasabah mengalami kerugian, sudah saatnya untuk menyusun aturan khusus mengenai transaksi mobile banking. Keamanan transaksi menjadi hal yang sangat penting, karena semakin banyaknya potensi risiko yang bisa terjadi, seperti penipuan atau kesalahan sistem. Karena itu, diperlukan regulasi yang jelas yang mengatur tanggung jawab bank dalam hal ini. Kedepannya, diharapkan Undang-Undang Perbankan dan peraturan-peraturan terkait dapat memberikan ketentuan yang lebih tegas lainnya dapat mencakup ketentuan yang lebih spesifik mengenai tanggung jawab bank dalam transaksi yang menggunakan sistem elektronik, seperti mobile banking. Aturan ini penting untuk mengatur hal-hal seperti bagaimana bank harus melindungi data nasabah, bagaimana mereka harus menangani gangguan atau masalah pada sistem, dan bagaimana mereka bertanggung jawab jika nasabah mengalami kerugian akibat kelalaian dari pihak bank.

Bukan hanya pihak bank saja tetapi diharapkan juga Bank Indonesia sebagai pengawas sektor perbankan diharapkan bisa meningkatkan pengawasannya terhadap bank-bank yang menyediakan layanan mobile banking. Pengawasan yang lebih ketat akan memastikan bahwa bank-bank tersebut mengikuti aturan yang berlaku, menjaga keamanan sistemnya, dan memberikan perlindungan yang maksimal bagi nasabah. Dengan adanya aturan yang lebih jelas dan pengawasan yang lebih baik, diharapkan transaksi mobile banking dapat berjalan dengan lebih aman dan nasabah mendapatkan perlindungan yang sesuai jika terjadi masalah (Made, 2020).

KESIMPULAN

Perlindungan hukum bagi pengguna mobile banking di tengah meningkatnya ancaman kejahatan siber dan kebocoran data pribadi. Dalam tulisan ini, menekankan bahwa meskipun terdapat sejumlah regulasi yang mengatur perlindungan hukum, Seperti Undang-Undang Perlindungan Konsumen serta peraturan dari Otoritas Jasa Keuangan (OJK) dan Bank Indonesia, penerapannya seringkali belum memadai untuk mengatasi tantangan yang timbul akibat kemajuan teknologi informasi. Perlindungan hukum dapat dibagi menjadi dua jenis, yaitu pencegahan atau preventif yang bertujuan untuk mencegah kerugian, dan represif yang fokus pada penanganan setelah kerugian terjadi. Namun, banyak nasabah yang masih kurang menyadari hak-hak mereka terkait perlindungan hukum tersebut. Di samping itu, tanggung jawab penyedia layanan mobile banking dalam menjaga keamanan data nasabah sangatlah krusial. Kegagalan dalam memberikan informasi yang akurat atau aman dapat menyebabkan kerugian bagi nasabah, sehingga penting bagi bank untuk memiliki prosedur yang jelas dalam menangani masalah ini. Penulis juga merekomendasikan agar regulasi yang ada perlu direvisi dan diperkuat demi memberikan perlindungan yang lebih baik bagi nasabah. Ini termasuk peningkatan transparansi informasi mengenai risiko yang dihadapi oleh pengguna layanan mobile banking serta penguatan mekanisme penyelesaian sengketa. Secara keseluruhan, jurnal ini menekankan bahwa meskipun sudah ada kerangka hukum, masih banyak aspek yang perlu diperbaiki untuk secara efektif melindungi nasabah mobile banking dari risiko cybercrime dan kebocoran data pribadi.

DAFTAR PUSTAKA

Akhmad, F. H., & Basuki, A. B. (2024, Juni). Upaya Hukum Bagi Korban Kejahatan Phising yang Menguras Saldo M-Banking. Jurnal Gagasan Hukum, Vol 6 (1).

Astrini, D. A. (2015, Januari-Maret). Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime. Lex Privatum, Vol III (1), 150.

Benedictus. (2022, Mei). Perlindungan Hukum Bagi Nasabah dan Bank Terhadap Tindak Kejahatan Berbasis Teknologi Informasi (Cyber Crime). Jurnal Hukum Caraka, Vol 2 (1).

Dewi, F. P., Widya, R. S., & Faricha, L. (2023, Desember). Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. Jurnal Ilmiah Ekonomi dan Manajemen, Vol 1 (4).

Irma, N. R., dkk. (2023, Juni). Pertanggungjawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah. Jurnal Pendidikan, Sosial dan Humaniora, Vol 3 (1).

Made, A. M. P. (2020). Tanggungjawab Hukum Bank Terhadap Nasabah dalam Hal Terjadinya Kegagalan Transaksi Pada Sistem Mobile Banking. Jurnal Kertha Wicaksana, Vol 14 (2).

Maulana, A. M & Apriani, R. (2021, September). Perlindungan Yuridis Terhadap Data Pribadi Nasabah Dalam Penggunaan Elektronik Banking (E-Banking). Jurnal Hukum De'rechstaat, Vol 7 (2).

Muhammad, I. S. P., Muhammad, H. S. & Revy, M. S. (2024, Januari). Penerapan Asas Kehati-Hatian Bank Untuk Perlindungan Hukum Bagi Nasabah Penyimpanan Dana. Jurnal Fakultas Hukum Lex Privatium, Vol 13 (1).

Nugraheni, T., Sinurat, A., & Kian, D. A. (2024, Juni). Analisis Yuridis Penerapan Perlindungan Hukum dalam Melindungi Pengguna Layanan Internet Banking dari Cyber Crime. Jurnal Hukum Politik dan Ilmu Sosial, Vol 3 (2).

Nunuk, S. (2008, September). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. Jurnal Ilmiah Hukum Dirgantar, Vol 9 (1).

See, B. R. (2022, Mei). Perlindungan Hukum Bagi Nasabah Bank Terhadap Tindak Kejahatan Berbasis Teknologi Informasi (CYBERCRIME). Jurnal Hukum Caraka Justitia, Vol 2 (3), 62-64.

Subaidah, R. J., Dhian, I. A., & Dian, S. (2023). Perlindungan Hukum Terhadap Nasabah Bank Korban Kejahatan Skimming. Jurnal USM Law Review, Vol 6 (1).

Tri, N., Aksi, S., & Darius, A. (2024, Juni). Analisis Yuridis Penerapan Perlindungan Hukum dalam Melindungi Pengguna Layanan Internet Banking dari Cyber Crime. Jurnal Hukum Politik dan Ilmu Sosial, Vol 3 (2).

Widayanti, P. W. (2022, Agustus). Tindak Pidana Data Nasabah Dalam Bidang Perbankan Sebagai Cybercrime. Legacy : Jurnal Hukum dan Perundang-undangan, Vol 2 (2), 14-15.

Yuslia. (2018). Pengaruh Penggunaan Internet Banking dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cyber Crime di Daerah Istimewa Yogyakarta. Jurnal Pendidikan dan Ekonomi, Vol 7 (6).

Zulina. (2024). Perlindungan Hukum Bagi Nasabah Bank Yang Dirugikan Dalam Transaksi Layanan M-Banking Dalam Kasus Kejahatan Dunia Maya (Cybercrime). Padang : Fakultas Hukum Universitas Bung Hatta.