Jurnal Retentum
Volume: 07, Number: 01, 2025, Page : 34-47
https://jurnal.darmaagung.ac.id/index.php/retentum

p-ISSN 2686-5432
e-ISSN 2686-5440

Pertanggungjawaban Bank dalam Menjamin Keamanan Data Nasabah di Era Digitalisasi Perbankan

Hanif Fonda[1], Zainal Arifin Hoesein[2]

[1,2]Universitas Borobudur
Email : hanifwta48@gmail.com[1*], zainal.arifin@umj.ac.id[2]

History:
Received : 05 Januari 2025
Revised : 10 Januari 2025
Accepted : 14 Januari 2025
Published: 15 Januari 2025

Publisher: Pascasarjana UDA

Abstrak

Penelitian ini bertujuan untuk menganalisis regulasi, perlindungan hukum, dan pertanggungjawaban bank terhadap keamanan data nasabah terhadap perkembangan perbankan digital di Indonesia. Fokus penelitian ini mencakup peraturan yang mengatur digitalisasi perbankan, seperti POJK No. 12/POJK.03/2018 dan POJK No. 12/POJK.03/2021, serta kekosongan hukum terkait perlindungan data pribadi nasabah dalam ekosistem digital. Penelitian juga mengkaji upaya perlindungan yang dilakukan oleh bank, baik melalui kebijakan internal seperti enkripsi data dan otentikasi berlapis, maupun mekanisme kompensasi bagi nasabah yang dirugikan akibat kejahatan siber. Penelitian ini juga membahas aspek pertanggungjawaban bank terhadap kerugian materiil yang dialami nasabah akibat kelalaian dalam menjaga keamanan data, serta kemungkinan tindakan hukum yang dapat diambil oleh nasabah, termasuk tuntutan perbuatan melawan hukum. Penelitian ini diharapkan dapat memberikan rekomendasi untuk penguatan regulasi dan mekanisme perlindungan yang lebih komprehensif dalam mengatasi tantangan yang muncul akibat digitalisasi perbankan.

Kata Kunci: Perbankan Digital, Keamanan Data Nasabah, Perlindungan Hukum, Regulasi Perbankan

Abstract

This study aims to analyze regulations, legal protection, and bank accountability for customer data security in relation to the development of digital banking in Indonesia. The focus of this study includes regulations governing banking digitalization, such as POJK No. 12/POJK.03/2018 and POJK No. 12/POJK.03/2021, as well as legal gaps related to the protection of customer personal data in the digital ecosystem. The study also examines the protection efforts made by banks, both through internal policies such as data encryption and layered authentication, as well as compensation mechanisms for customers who are harmed by cybercrime. This study also discusses aspects of bank accountability for material losses experienced by customers due to negligence in maintaining data security, as well as possible legal actions that can be taken by customers, including lawsuits for unlawful acts. This study is expected to provide recommendations for strengthening regulations and more comprehensive protection mechanisms in overcoming the challenges that arise due to banking digitalization.

Keywords: *Digital Banking, Customer Data Security, Legal Protection, Banking Regulation*

Jurnal Retentum
Volume: 07, Number: 01, 2025, Page : 34-47
https://jurnal.darmaagung.ac.id/index.php/retentum
p-ISSN 2686-5432
e-ISSN 2686-5440

PENDAHULUAN

Perbankan digital telah mengalami transformasi yang signifikan dalam beberapa tahun terakhir didorong oleh kemajuan teknologi informasi yang memungkinkan aksesibilitas layanan perbankan yang lebih baik, cepat, dan efisien (Ngamal & Perajaka, 2021). Sebelumnya layanan perbankan umumnya dilakukan melalui interaksi langsung di cabang bank atau menggunakan media fisik seperti buku tabungan dan cek. Dengan kemunculan teknologi digital paradigma perbankan telah bergeser ke ranah digital melalui berbagai platform seperti internet banking, mobile banking, dan bank digital yang sepenuhnya beroperasi secara online tanpa kehadiran cabang fisik (Alfarizi et al., 2023). Pendorong utama dari perkembangan perbankan digital ini adalah kebutuhan masyarakat akan layanan yang lebih cepat, praktis, dan efisien. Dengan adanya teknologi mobile dan internet masyarakat kini dapat melakukan berbagai transaksi perbankan kapan saja dan di mana saja tanpa harus mengunjungi bank fisik. Kemajuan dalam sistem pembayaran digital seperti e-wallet, QR code, dan teknologi pembayaran nirsentuh (contactless) semakin memudahkan konsumen dalam melakukan pembayaran, transfer uang, serta pembelian produk atau layanan tanpa batasan waktu dan lokasi (Priambodo et al., 2022). Kemajuan teknologi ini tidak hanya meningkatkan aksesibilitas perbankan bagi masyarakat urban tetapi juga membuka peluang bagi masyarakat di daerah terpencil yang sebelumnya mengalami kesulitan dalam mengakses layanan perbankan tradisional.

Sebelum adanya perbankan digital transaksi perbankan umumnya dilakukan secara langsung di cabang bank dengan menggunakan media fisik seperti buku tabungan, cek, atau uang tunai (Akbar, 2023). Nasabah diwajibkan untuk hadir di bank guna melaksanakan berbagai transaksi, termasuk setoran, penarikan, transfer, dan pembayaran tagihan. Proses ini sering kali memakan waktu dan memerlukan kehadiran fisik baik dari pihak nasabah maupun petugas bank. Keterbatasan waktu operasional bank dan lokasi cabang juga menjadi hambatan bagi banyak individu, terutama bagi mereka yang tinggal di daerah terpencil (Marlina & Bimo, 2018).

Kemunculan perbankan digital masyarakat kini semakin terbiasa melakukan transaksi perbankan melalui platform daring seperti mobile banking dan internet banking. Berbagai aktivitas perbankan yang sebelumnya memerlukan kehadiran fisik kini dapat dilaksanakan dengan mudah melalui aplikasi di ponsel atau komputer (Rizieq & Suwarsit, 2024). Nasabah dapat melakukan transfer antarbank, membayar tagihan, membeli produk atau layanan, bahkan berinvestasi semuanya hanya dengan beberapa kali klik. Perubahan ini telah mengubah pola transaksi dari yang konvensional menjadi lebih praktis, cepat, dan efisien. Kemudahan yang ditawarkan oleh perbankan digital memungkinkan nasabah untuk melakukan transaksi kapan saja dan di mana saja, tanpa terikat oleh jam operasional bank atau lokasi cabang (D. C. P. Putri & Lutfianti,

2024). Hal ini sangat menguntungkan bagi mereka yang memiliki jadwal padat atau yang tinggal jauh dari cabang bank. Dengan adanya aplikasi perbankan, transaksi seperti transfer antarbank, pembayaran tagihan, atau pembelian produk dapat dilakukan dalam hitungan detik.

Kecepatan transaksi yang ditawarkan oleh perbankan digital juga menjadi salah satu faktor utama yang mendorong adopsi teknologi ini. Sebagai contoh, transfer dana antarbank yang dulunya memerlukan waktu berhari-hari atau bahkan beberapa jam kini dapat diselesaikan dalam hitungan menit (Purba et al., 2020). Sistem pembayaran digital memungkinkan nasabah untuk melakukan pembayaran dalam jumlah besar dengan cepat dan aman, yang sebelumnya sulit dilakukan menggunakan cek atau uang tunai.

Meskipun kemudahan dan kecepatan ini membawa manfaat besar, tantangan baru juga muncul terutama terkait keandalan sistem dan risiko penyalahgunaan teknologi. Sistem perbankan digital harus senantiasa dalam kondisi andal untuk menghindari gangguan yang dapat merugikan nasabah. Keamanan data nasabah menjadi isu krusial karena transaksi yang dilakukan secara digital rentan terhadap ancaman peretasan atau pencurian data (Antoine et al., 2025). Oleh karena itu, meskipun perbankan digital menawarkan kenyamanan, penting bagi bank untuk terus meningkatkan keandalan dan keamanan sistem mereka agar risiko penyalahgunaan teknologi dapat diminimalkan.

Perkembangan pesat perbankan digital telah memberikan dampak signifikan terhadap aksesibilitas dan efisiensi layanan perbankan, namun juga menghadirkan tantangan dalam hal regulasi hukum yang ada. Meskipun sektor perbankan diatur oleh berbagai peraturan, seperti Undang-Undang Perbankan dan regulasi dari Otoritas Jasa Keuangan (OJK), banyak aspek terkait dengan perbankan digital yang belum sepenuhnya tercakup dalam ketentuan hukum yang berlaku. Sebagai contoh, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan belum diperbarui untuk memasukkan unsur digitalisasi dalam sektor perbankan, sehingga regulasi yang ada masih terbatas dalam menangani isu-isu yang muncul akibat kemajuan teknologi (Tarigan & Paulus, 2019).

Sebagai respons terhadap perkembangan ini, pemerintah melalui Bank Indonesia dan OJK telah mengeluarkan kebijakan yang bertujuan untuk memberikan jaminan kepastian hukum dan perlindungan bagi nasabah. Salah satu kebijakan tersebut adalah Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum, yang memberikan pedoman mengenai layanan perbankan elektronik dan aspek pengamanan data nasabah (Abubakar & Handayani, 2022). Namun, peraturan ini masih belum mencakup secara komprehensif seluruh aspek terkait potensi risiko dan tantangan hukum yang muncul dalam implementasi perbankan digital. Di sisi lain kejahatan siber yang berkaitan dengan perbankan digital menjadi tantangan besar dalam penegakan hukum. Tindakan ilegal seperti peretasan akun nasabah, penipuan digital, dan pencurian data

sering kali sulit ditangani dengan hukum yang ada (Evi, 2023). Dengan semakin kompleksnya teknologi, tindakan-tindakan ini sering dilakukan dengan cara yang tersembunyi dan sulit dilacak, sehingga menyulitkan proses penegakan hukum.

Dalam banyak kasus nasabah yang menjadi korban serangan dunia maya sering kali merasa dirugikan, namun perlindungan hukum yang ada belum memadai untuk melindungi mereka. Bank sebagai penyedia layanan perbankan digital juga menghadapi tantangan besar karena berisiko menghadapi tuntutan hukum dari nasabah yang mengalami kerugian akibat kejahatan siber (Risqiana et al., 2024). Meskipun Peraturan OJK telah memberikan pedoman mengenai kewajiban pengamanan data nasabah, bank sering kali terjebak dalam posisi sulit terkait pertanggungjawaban atas kerugian yang dialami nasabah akibat peretasan atau kebocoran data. Sehingga pengembangan regulasi yang lebih spesifik mengenai perlindungan nasabah dan pertanggungjawaban bank terhadap kejahatan siber menjadi sangat penting.

Tantangan hukum yang terkait dengan perbankan digital mencakup kesulitan dalam pembuktian dan penanggulangan kejahatan siber. Mayoritas transaksi dilakukan secara elektronik, yang menambah kompleksitas dalam pembuktian apabila terjadi tindak pidana. Kejahatan siber seperti peretasan akun nasabah dan pencurian data, sering kali sulit dilacak, terutama ketika pelaku memanfaatkan teknologi untuk menghilangkan jejak digital mereka (Dharani, 2024). Dalam hal ini, Peraturan OJK menyatakan bahwa layanan bank digital harus mengoptimalkan pemanfaatan data nasabah; namun, di sisi lain, hal ini juga meningkatkan risiko pencurian data jika pengamanan tidak dilaksanakan dengan baik.

Seiring dengan pesatnya perkembangan perbankan digital, bank dituntut untuk segera memperbaiki dan meningkatkan sistem pengamanan data guna mengurangi risiko kejahatan siber. Oleh karena itu, pembaruan regulasi hukum yang lebih spesifik mengenai keamanan data nasabah sangat diperlukan, sebagaimana diatur dalam Pasal 239 UU Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, yang mewajibkan Penyelenggara Usaha Sistem Keuangan (PUSK) untuk menjaga kerahasiaan dan keamanan data nasabah (Kartiko et al., 2024). Meskipun terdapat kewajiban tersebut, tantangan terbesar terletak pada bagaimana mengimplementasikan pengaturan ini secara efektif agar kejahatan siber dapat diminimalisir dan perlindungan hukum bagi nasabah dapat terjamin dengan baik.

Keamanan data nasabah dalam transaksi digital merupakan isu yang sangat krusial di tengah pesatnya perkembangan perbankan digital. Dalam ekosistem ini data nasabah yang bersifat pribadi dan sensitif rentan terhadap risiko kebocoran atau penyalahgunaan oleh pihak yang tidak bertanggung jawab. Sehingga penelitian lebih lanjut diperlukan untuk menganalisis peraturan yang ada, menilai efektivitasnya, dan mengidentifikasi celah-celah yang memungkinkan terjadinya pelanggaran. Hal ini penting agar bank dan lembaga keuangan dapat memastikan

perlindungan maksimal bagi nasabah, serta meningkatkan kepercayaan masyarakat terhadap layanan perbankan digital.

Selain mengidentifikasi kekurangan dalam regulasi yang ada, penelitian juga harus diarahkan untuk memberikan rekomendasi perbaikan, baik dalam bentuk pembaruan peraturan maupun penguatan mekanisme perlindungan hukum. Dengan adanya penelitian ini, regulasi yang lebih spesifik dan relevan terhadap dinamika perbankan digital dapat dirumuskan untuk menutup celah hukum yang ada. Rekomendasi tersebut juga dapat mencakup langkah-langkah preventif yang lebih efektif, seperti pengawasan ketat oleh regulator, penerapan teknologi keamanan yang canggih, serta prosedur yang jelas dalam menangani sengketa dan kerugian yang dialami nasabah.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yang berfokus pada kajian terhadap norma-norma hukum yang berlaku, terutama yang berkaitan dengan regulasi perlindungan jurnalistik dan kebebasan pers di Indonesia. Pendekatan yang digunakan dalam penelitian ini adalah statute approach, yang mengutamakan analisis terhadap peraturan perundang-undangan yang ada, seperti Undang-Undang Pers dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), untuk memahami bagaimana regulasi tersebut mengatur kebebasan pers serta perlindungan terhadap jurnalis. Penelitian ini juga menggunakan comparative approach, yang membandingkan regulasi perlindungan jurnalistik di Indonesia dengan sistem hukum di negara lain yang memiliki pendekatan serupa dalam melindungi kebebasan pers, guna memperoleh perspektif yang lebih luas mengenai kelemahan, tantangan, serta potensi rekonstruksi regulasi yang berbasis nilai keadilan. Pendekatan ini memungkinkan peneliti untuk mengevaluasi efektivitas regulasi yang ada dan memberikan rekomendasi untuk perbaikan regulasi yang lebih adil dan efektif dalam mendukung kebebasan pers dan perlindungan terhadap jurnalis di Indonesia.

HASIL DAN PEMBAHASAN

Kekosongan Hukum Mengenai Regulasi Digitalisasi Perbankan Indonesia Serta Perlindungan Hukum bagi Nasabah dalam Digital Perbankan

Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum merupakan salah satu regulasi yang mengatur perbankan digital di Indonesia. Dalam peraturan ini, layanan perbankan digital didefinisikan sebagai layanan yang memungkinkan nasabah untuk memperoleh informasi, berkomunikasi, dan melakukan transaksi perbankan melalui media elektronik (Tarantang et al., 2023). Layanan ini dirancang untuk memberikan pengalaman yang lebih cepat, mudah, dan sesuai dengan kebutuhan nasabah (customer experience). POJK ini juga mencakup ruang lingkup pengaturan yang meliputi pengoptimalan pemanfaatan data nasabah guna meningkatkan efisiensi layanan perbankan. Aspek pengamanan menjadi perhatian utama dalam peraturan ini, di mana bank diwajibkan untuk memastikan keamanan data

nasabah dalam setiap proses transaksi digital. Namun, pengaturan mengenai mekanisme keamanan data tersebut masih bersifat umum dan belum memberikan rincian teknis tentang langkah-langkah mitigasi risiko keamanan yang dapat diterapkan oleh bank.

Peraturan Otoritas Jasa Keuangan (POJK) Nomor 12/POJK.03/2021 tentang Bank Umum juga berfungsi sebagai landasan penting dalam proses digitalisasi perbankan. Regulasi ini menekankan perlunya adaptasi perbankan terhadap perkembangan teknologi informasi dan digitalisasi (Pratama, 2021). Salah satu fokus utama dari POJK ini adalah mendorong bank untuk melakukan transformasi digital yang lebih inklusif, sehingga dapat menjangkau masyarakat luas, termasuk mereka yang belum memiliki akses ke layanan perbankan konvensional. Bank diwajibkan untuk menyediakan infrastruktur teknologi informasi yang memadai guna mendukung layanan perbankan digital. Bank juga diharuskan untuk memiliki manajemen risiko yang baik dalam menghadapi ancaman siber. Meskipun demikian, regulasi ini belum memberikan panduan teknis yang rinci mengenai cara pengelolaan risiko keamanan siber dan langkah-langkah perlindungan yang harus diterapkan oleh bank untuk melindungi nasabah dari potensi ancaman kejahatan digital.

Meskipun Peraturan Otoritas Jasa Keuangan (POJK) Nomor 12/POJK.03/2018 dan POJK Nomor 12/POJK.03/2021 menekankan pentingnya keamanan data nasabah pengaturan yang ada masih bersifat umum. Saat ini belum terdapat aturan teknis yang spesifik mengenai langkah-langkah perlindungan data, seperti kewajiban enkripsi, otentikasi dua faktor, atau manajemen akses data. Hal ini menciptakan celah yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan kejahatan siber. Hingga saat ini idak ada pengaturan yang secara jelas menetapkan mekanisme tanggung jawab bank apabila terjadi kejahatan siber yang merugikan nasabah. Ini mencakup tanggung jawab bank untuk memberikan kompensasi atas kerugian materiil, langkah mitigasi yang harus diambil, serta perlindungan hukum bagi nasabah yang menjadi korban. Tanpa adanya pengaturan yang jelas, nasabah sering kali berada dalam posisi yang lemah ketika menghadapi kerugian akibat kejahatan digital.

Regulasi yang ada belum sepenuhnya terintegrasi dengan Undang-Undang Perlindungan Data Pribadi atau regulasi lain yang relevan. Situasi ini menyebabkan adanya tumpang tindih kewenangan dan potensi konflik hukum dalam pelaksanaan perlindungan nasabah di sektor perbankan digital. Oleh karena itu, diperlukan langkah-langkah untuk memperkuat kerangka hukum agar dapat memberikan perlindungan yang lebih efektif bagi nasabah serta memastikan tanggung jawab bank dalam menghadapi risiko-risiko tersebut.

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang merupakan amandemen terhadap Undang-Undang Nomor 7 Tahun 1992, berfungsi sebagai dasar hukum utama bagi sistem perbankan di Indonesia. Namun, undang-undang ini belum mengalami pembaruan signifikan untuk

mengakomodasi perkembangan teknologi digital yang berdampak pada sektor perbankan. Akibatnya, terdapat kekosongan hukum, terutama dalam pengaturan layanan perbankan berbasis teknologi, seperti penggunaan aplikasi digital, pemanfaatan big data, dan keamanan siber. Digitalisasi layanan perbankan telah menciptakan pola transaksi baru yang melibatkan otomatisasi dan penerapan teknologi canggih. Sayangnya, UU Perbankan yang ada belum secara eksplisit mengatur aspek-aspek penting, seperti kewajiban bank untuk memastikan keamanan transaksi elektronik, perlindungan data nasabah secara rinci, serta mekanisme penyelesaian sengketa yang timbul akibat kejahatan siber (Hendarto & Prasetyawati, 2024). Ketiadaan pengaturan ini menimbulkan potensi kerugian bagi nasabah, terutama dalam kasus kebocoran data atau penipuan digital.

Salah satu aspek yang sangat penting dalam perbankan digital adalah perlindungan data nasabah. Di Indonesia perlindungan data pribadi telah diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) (Suryanto et al., 2024). Perlu diketahui bahwa undang-undang ini bersifat umum dan tidak secara spesifik mengatur pelaksanaan perlindungan data nasabah di sektor perbankan.Regulasi yang ada, seperti Peraturan Otoritas Jasa Keuangan (POJK) dan Surat Edaran Bank Indonesia, belum memberikan pedoman teknis yang memadai terkait keamanan data nasabah. Sebagai contoh, belum terdapat kewajiban rinci mengenai penerapan teknologi enkripsi, sertifikasi keamanan digital, atau prosedur audit keamanan siber bagi bank. Kekurangan ini membuat nasabah rentan terhadap ancaman, seperti kebocoran data atau pencurian identitas, tanpa adanya jaminan perlindungan yang memadai dari pihak bank.

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menegaskan tanggung jawab bank untuk melindungi dana dan informasi nasabah. Regulasi ini mengharuskan bank untuk menjaga kerahasiaan data nasabah serta mencegah penyalahgunaan informasi (Dewi & Wiyanti, 2024). Undang-undang ini memiliki keterbatasan dalam mengatur mengenai digitalisasi perbankan terutama dalam mengatur risiko yang muncul dari teknologi digital, seperti kebocoran data atau kejahatan siber, yang belum diakomodasi secara eksplisit. Di sisi lain Undang-Undang Perlindungan Konsumen memberikan hak kepada konsumen untuk mendapatkan informasi yang jujur, perlakuan adil, dan perlindungan keamanan (Mewu & Mahadewi, 2023). Mengenai digitalisasi perbankan hak ini relevan untuk menjamin transparansi bank dalam memberikan layanan dan perlindungan terhadap risiko siber. Meskipun demikian, penerapannya masih memerlukan penyesuaian karena tantangan yang dihadapi dalam teknologi digital sering kali tidak tercakup dalam regulasi yang lebih umum ini.

Sementara itu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mengatur tentang keamanan informasi digital dan memberikan dasar hukum untuk menangani kejahatan siber (Ramadhani, 2023). Peraturan ini

berfungsi sebagai landasan untuk mengatur perlindungan data nasabah serta tindakan terhadap pelaku kejahatan digital. Dalam penerapan UU ITE mengenai perbankan masih menghadapi kendala, seperti kurangnya spesifikasi mengenai mekanisme tanggung jawab bank terhadap kerugian nasabah akibat serangan siber. Peraturan Otoritas Jasa Keuangan (POJK) juga mewajibkan penyedia jasa keuangan, termasuk bank, untuk melindungi konsumen dengan menjaga keamanan data nasabah, memberikan layanan yang adil, dan menyediakan mekanisme pengaduan. Fokus utama dari regulasi ini adalah pengamanan data nasabah melalui standar operasional tertentu dan edukasi konsumen. Namun, efektivitasnya sering kali bergantung pada implementasi oleh masing-masing lembaga keuangan.

Pertanggungjawaban Bank Terhadap Keamanan Data Nasabah serta Isu Keamanan Data dan Kejahatan Siber dalam Perbankan Digital

Tanggung jawab bank diatur oleh Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan berbagai peraturan yang dikeluarkan oleh Otoritas Jasa Keuangan (OJK). Dalam undang-undang ini ditegaskan bahwa bank memiliki kewajiban untuk menjaga kepercayaan nasabah dengan melindungi dana dan informasi mereka. Kewajiban ini mencakup pengelolaan risiko yang muncul dalam layanan digital, seperti serangan siber dan kebocoran data. Tanggung jawab bank mengikuti prinsip hukum perdata, di mana bank dapat dimintai pertanggungjawaban atas kelalaian yang menyebabkan kerugian materiil bagi nasabah (D. F. Putri et al., 2023). Kelalaian bank, seperti lemahnya pengamanan data atau kegagalan dalam sistem layanan digital, dapat dianggap sebagai pelanggaran kontraktual. Hal ini membuka peluang bagi nasabah untuk mengajukan gugatan terhadap bank jika terjadi kerugian akibat kelalaian tersebut.

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU PPSK) memperkuat kewajiban bank dalam melindungi data nasabah. Pasal 239 UU PPSK menetapkan bahwa lembaga jasa keuangan, termasuk bank, wajib menjaga kerahasiaan, keamanan, dan integritas data nasabah dengan memanfaatkan teknologi informasi yang andal. Bank harus memastikan bahwa data nasabah tidak disalahgunakan atau diakses oleh pihak yang tidak berwenang. Apabila terjadi pelanggaran, bank dapat dikenakan sanksi administratif dan diwajibkan untuk memberikan ganti rugi kepada nasabah.

Bank juga memiliki kewajiban proaktif dalam melindungi keamanan data nasabah. Hal ini mencakup penerapan sistem pengamanan data berlapis, melakukan audit keamanan secara berkala, serta mengembangkan prosedur manajemen risiko yang komprehensif. Upaya ini menjadi semakin penting mengingat meningkatnya kasus kejahatan siber yang menargetkan lembaga perbankan. Bank diwajibkan untuk memberikan edukasi kepada nasabah mengenai pentingnya menjaga keamanan data pribadi mereka, seperti penggunaan otentikasi berlapis dan menghindari berbagi informasi sensitif melalui saluran yang tidak aman.

Kelalaian bank dalam pengamanan data nasabah merupakan pelanggaran serius yang dapat dimintai pertanggungjawaban hukum berdasarkan Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) mengenai perbuatan melawan hukum (PMH). Pasal ini menetapkan bahwa setiap tindakan melawan hukum yang menyebabkan kerugian pada orang lain mengharuskan pelaku untuk memberikan ganti rugi. Kelalaian bank dapat mencakup kegagalan dalam menyediakan sistem keamanan yang memadai, kurangnya langkah mitigasi risiko, atau ketidakmampuan mencegah akses ilegal ke data nasabah. Sebagai contoh, kebocoran data akibat lemahnya enkripsi atau serangan siber yang tidak dapat ditangkal menunjukkan kelalaian bank dalam melindungi informasi sensitif nasabah. Nasabah yang mengalami kerugian akibat kelalaian bank memiliki beberapa mekanisme hukum untuk mengajukan gugatan. Mereka dapat mengajukan gugatan perdata berdasarkan PMH secara individu atau melalui gugatan kelompok (class action) jika banyak nasabah mengalami kerugian yang serupa. Dalam gugatan tersebut nasabah harus membuktikan adanya kelalaian dari pihak bank, kerugian yang timbul, serta hubungan sebab-akibat antara keduanya. Misalnya, jika kebocoran data menyebabkan pencurian identitas yang merugikan nasabah secara finansial, bank dapat dimintai pertanggungjawaban.

Proses hukum ini juga didukung oleh regulasi yang dikeluarkan oleh Otoritas Jasa Keuangan (OJK), yang memberikan panduan bagi nasabah dalam menyelesaikan sengketa melalui mediasi atau arbitrase jika tidak ingin membawa kasus ke pengadilan (Mairul & Dewi, 2018). Gugatan kelompok menjadi salah satu mekanisme penting, terutama ketika kasus melibatkan sejumlah besar nasabah yang mengalami kerugian akibat pelanggaran sistemik, seperti pelanggaran kebijakan privasi atau kegagalan bank dalam menangani serangan siber. Bank yang terbukti melanggar kewajiban hukum dalam melindungi data nasabah dapat dikenakan berbagai sanksi sesuai dengan peraturan perundang-undangan.Secara administratif, sanksi dapat berupa denda, pencabutan izin usaha, atau perintah untuk memperbaiki sistem keamanan yang tidak memadai.

Sanksi ini diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan peraturan OJK seperti POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen. Jika kelalaian bank terbukti sebagai perbuatan melawan hukum, bank dapat dikenakan sanksi perdata berupa kewajiban untuk memberikan ganti rugi kepada nasabah. Dalam kasus tertentu terutama jika kebocoran data menimbulkan kerugian besar dan dilakukan dengan kesengajaan, bank juga dapat dikenakan sanksi pidana berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Sanksi pidana ini dapat mencakup hukuman denda yang signifikan atau bahkan hukuman penjara bagi individu di dalam manajemen bank yang terbukti bertanggung jawab.

Kejahatan siber menjadi ancaman yang semakin nyata, dengan berbagai metode yang digunakan oleh pelaku untuk meretas data nasabah atau mengakses dana secara ilegal. Beberapa jenis kejahatan siber yang sering terjadi

di sektor ini mencakup phishing, malware, ransomware, dan pencurian identitas digital. Phishing adalah metode penipuan di mana pelaku mengirimkan email atau pesan palsu yang tampaknya berasal dari lembaga perbankan atau perusahaan terpercaya. Tujuan dari tindakan ini adalah untuk memperoleh informasi sensitif seperti username, password, atau nomor kartu kredit nasabah. Pelaku biasanya menggunakan situs web palsu yang menyerupai situs perbankan resmi untuk mencuri data pribadi nasabah.

Malware merupakan jenis kejahatan yang melibatkan perangkat lunak berbahaya yang diinstal pada perangkat nasabah tanpa sepengetahuan mereka. Perangkat ini kemudian digunakan untuk mengakses informasi pribadi atau mengendalikan perangkat tersebut untuk melakukan transaksi ilegal. Malware dapat berupa virus, trojan, atau spyware yang dapat mencuri data atau memonitor aktivitas online nasabah. Ransomware adalah jenis kejahatan di mana perangkat lunak mengenkripsi data pada perangkat korban dan meminta tebusan agar data tersebut dapat dibuka kembali. Pelaku dapat mengenkripsi data penting nasabah atau bank dan mengancam akan menghancurkan atau membocorkannya jika tidak ada pembayaran.

Pencurian identitas digital terjadi ketika pelaku memperoleh informasi pribadi nasabah, seperti nomor rekening, PIN, atau informasi login lainnya, dan menggunakannya untuk melakukan transaksi yang merugikan nasabah. Tindakan ini dapat dilakukan melalui peretasan akun-akun perbankan digital atau pengumpulan data melalui metode ilegal seperti social engineering.

Kerentanan sistem perbankan digital terhadap ancaman siber dipengaruhi oleh berbagai faktor, baik internal maupun eksternal. Salah satu faktor utama yang meningkatkan risiko serangan siber adalah teknologi yang tidak memadai. Meskipun banyak bank telah mengadopsi sistem digital modern, tidak semua bank memiliki infrastruktur keamanan yang kuat dan mutakhir untuk menangkal serangan siber. Sistem yang ketinggalan zaman atau tidak diperbarui secara berkala menjadi sasaran empuk bagi para hacker yang mencari celah untuk menembus pertahanan bank.

Rendahnya kesadaran nasabah terhadap pentingnya keamanan digital juga berkontribusi pada meningkatnya risiko kejahatan siber. Banyak nasabah yang belum sepenuhnya memahami cara melindungi akun perbankan mereka, seperti pentingnya menggunakan kata sandi yang kuat, menghindari tautan mencurigakan, dan memverifikasi keaslian komunikasi dari bank. Faktor-faktor ini memberikan ruang bagi pelaku kejahatan untuk mengeksploitasi ketidaktahuan nasabah melalui teknik phishing atau malware yang menargetkan kelemahan individu. Kerentanan dalam sistem otentikasi juga menjadi masalah signifikan. Penggunaan kata sandi yang lemah atau ketergantungan pada otentikasi berbasis satu faktor dapat mempermudah akses ilegal ke akun nasabah. Sistem perbankan digital yang belum menerapkan otentikasi multi-faktor atau lapisan keamanan ganda juga rentan terhadap serangan. Oleh karena itu, bank perlu secara proaktif meningkatkan teknologi keamanan mereka serta memberikan pelatihan dan

edukasi kepada nasabah mengenai cara menjaga data pribadi mereka tetap aman.

Nasabah yang merasa dirugikan akibat kejahatan siber yang timbulm karena adanya perbankan digital memiliki hak untuk mengajukan pengaduan melalui berbagai saluran yang disediakan oleh bank atau lembaga terkait. Proses pengaduan dimulai dengan nasabah melaporkan insiden yang terjadi, seperti pencurian data atau transaksi yang tidak sah, kepada bank tempat mereka membuka rekening. Bank kemudian akan memproses laporan ini dan melakukan penyelidikan awal untuk menentukan apakah terdapat pelanggaran terhadap kebijakan atau kelalaian dalam prosedur keamanan yang diterapkan. Otoritas Jasa Keuangan (OJK) memainkan peran penting dalam mediasi sengketa antara bank dan nasabah. Sebagai lembaga pengawas sektor keuangan di Indonesia, OJK menyediakan saluran pengaduan bagi nasabah yang merasa hak-haknya dilanggar oleh penyedia jasa keuangan, termasuk bank.

OJK bertanggung jawab untuk memfasilitasi penyelesaian sengketa secara adil, dengan tujuan melindungi kepentingan nasabah serta memastikan kepatuhan bank terhadap regulasi yang berlaku. Proses mediasi ini bertujuan untuk menemukan solusi yang memadai bagi pihak-pihak yang bersengketa, dengan memberikan rekomendasi atau keputusan yang dapat dilaksanakan oleh pihak bank.Dalam hal kompensasi bagi nasabah yang mengalami kerugian, OJK mengatur mekanisme pemberian kompensasi bagi nasabah yang menderita kerugian akibat kelalaian atau kesalahan bank dalam menjaga keamanan data atau transaksi. Bank diwajibkan untuk bertanggung jawab atas kerugian yang ditimbulkan akibat peristiwa tersebut dan melakukan penggantian sesuai dengan ketentuan yang berlaku dalam Peraturan Otoritas Jasa Keuangan (POJK) Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen. Nasabah yang menjadi korban kejahatan siber dapat mengajukan klaim kompensasi yang harus diselesaikan oleh bank, dengan mempertimbangkan besarnya kerugian yang dialami serta bukti yang disediakan oleh nasabah.

Bank dapat memanfaatkan media sosial sebagai alat strategis untuk membangun kepercayaan nasabah dengan beberapa cara yang efektif. Pertama, media sosial memungkinkan bank untuk meningkatkan kesadaran merek dan keterlibatan nasabah. Dengan menggunakan platform seperti Facebook, Instagram, dan Twitter bank dapat menjangkau audiens yang lebih luas dan menyampaikan informasi tentang produk serta layanan mereka secara langsung. Hal ini tidak hanya meningkatkan pengenalan merek tetapi juga membantu bank bersaing lebih efektif di pasar yang semakin kompetitif.

Kedua, konten edukatif yang disajikan melalui media sosial memainkan peran penting dalam meningkatkan pemahaman nasabah tentang produk dan layanan bank. Dengan menyediakan informasi yang jelas dan mudah dipahami mengenai prinsip-prinsip produk, manfaatnya, serta cara penggunaannya, bank dapat membantu nasabah membuat keputusan keuangan yang lebih baik. Konten seperti artikel, video tutorial, dan infografis tidak hanya menarik perhatian

tetapi juga membangun kredibilitas bank sebagai sumber informasi yang terpercaya.

Ketiga, interaksi personal melalui media sosial sangat penting dalam membangun hubungan yang kuat antara bank dan nasabah. Dengan berkomunikasi secara langsung dan responsif, bank dapat menjawab pertanyaan nasabah serta memberikan dukungan yang diperlukan. Penelitian menunjukkan bahwa interaksi ini dapat menciptakan pengalaman positif bagi nasabah, yang pada akhirnya berkontribusi pada peningkatan loyalitas.

Keempat, transparansi dalam komunikasi juga dapat diperoleh melalui penggunaan media sosial. Dengan membagikan informasi terkait kegiatan bank, laporan keuangan, dan berita terbaru tentang produk, bank dapat meningkatkan kepercayaan nasabah. Kepercayaan adalah faktor kunci dalam hubungan perbankan; dengan memberikan informasi yang transparan, bank menunjukkan komitmennya terhadap integritas dan akuntabilitas.

Akhirnya, kampanye komunikasi yang menyoroti fitur keamanan dan manfaat penggunaan layanan digital juga dapat membantu membangun kepercayaan nasabah. Menampilkan testimoni pelanggan yang puas berfungsi sebagai bukti sosial yang meyakinkan calon pengguna untuk mencoba layanan tersebut. Dengan strategi komunikasi yang tepat dan penggunaan media sosial secara efektif, bank dapat menciptakan hubungan jangka panjang dengan nasabah serta meningkatkan kepuasan dan loyalitas mereka

SIMPULAN

Regulasi yang mengatur perbankan digital di Indonesia, seperti Peraturan Otoritas Jasa Keuangan (POJK) dan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, menekankan pentingnya perlindungan data nasabah dan pengelolaan risiko yang muncul akibat digitalisasi. Meskipun terdapat kewajiban bagi bank untuk menjaga keamanan dan kerahasiaan data nasabah, pengaturan yang ada masih bersifat umum dan kurang memberikan rincian teknis mengenai langkah-langkah mitigasi risiko, sehingga menciptakan celah yang dapat dimanfaatkan oleh pelaku kejahatan siber. Kelalaian bank dalam melindungi data nasabah dapat mengakibatkan pertanggungjawaban hukum dan sanksi administratif. Oleh karena itu, diperlukan penguatan kerangka hukum yang lebih spesifik dan komprehensif untuk memastikan perlindungan nasabah yang lebih efektif serta meningkatkan kesadaran akan keamanan digital, baik dari pihak bank maupun nasabah itu sendiri.

Tanggung jawab bank dalam melindungi data nasabah diatur oleh berbagai regulasi, termasuk Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, yang menekankan pentingnya menjaga kerahasiaan dan keamanan data. Kelalaian bank dalam pengamanan data dapat mengakibatkan pertanggungjawaban hukum, di mana nasabah berhak mengajukan gugatan jika mengalami kerugian akibat tindakan melawan hukum. Dalam menghadapi

ancaman siber yang semakin meningkat, bank perlu menerapkan sistem keamanan yang kuat, memberikan edukasi kepada nasabah, serta memanfaatkan media sosial untuk membangun kepercayaan melalui transparansi dan interaksi yang baik. Dengan demikian, upaya ini tidak hanya melindungi nasabah tetapi juga.

DAFTAR PUSTAKA

Abubakar, L., & Handayani, T. (2022). PENGUATAN REGULASI: UPAYA PERCEPATAN TRANSFORMASI DIGITAL PERBANKAN DI ERA EKONOMI DIGITAL. Masalah-Masalah Hukum, 51(3), 259–270. https://doi.org/10.14710/mmh.51.3.2022.259-270

Akbar, M. R. (2023). Perkembangan yang Pesat dan Tantangan yang Dihadapi oleh Perbankan Digital di Indonesia. Ecobankers : Journal of Economy and Banking, 4(2), 95–111. https://jurnal.uibbc.ac.id/index.php/EcoBankers/article/view/989

Alfarizi, M., Kamila Hanum, R., Firmansyah, A. A., & Wusqo, U. (2023). Digital Banking dalam Akselerasi Pemberdayaan Ekonomi Womenpreneur Indonesia : Eksplorasi Sosial-Ekonomi dan Peran LPS Berbasis PLS-SEM. Jurnal Magister Ekonomi Syariah, 2(2 Desember), 1–32. https://doi.org/10.14421/jmes.2023.022-01

Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia). JMIA : Jurnal Multidisiplin Ilmu Akademik, 2(1), 316–327.

Dewi, R. P., & Wiyanti, D. (2024). Perlindungan Hukum Nasabah atas Peretasan Data Pribadi ditinjau dari Undang Undang. Jurnal RIset Ilmu Hukum (JRIH), 4(2), 95–100.

Dharani, L. I. C. (2024). Perlindungan Hukum terhadap Tindakan Phishing di Media Sosial. Penerbit NEM.

Evi, T. (2023). TRANSFORMASI TRANSAKSI TUNAI KE DIGITAL DI INDONESIA. CV. AA. Rizky.

Hendarto, V. A., & Prasetyawati, E. (2024). Tanggung Jawab Bank Dalam Mengantisipasi Dan Menangani Kerugian Nasabah Akibat Scam Melalui Link Phising Pada Mobile Banking. Iuris Studia: Jurnal Kajian Hukum, 5(3), 759–765.

Kartiko, N. D., Soegiono, S. P., Siswanto, C. A., & Indradewi, A. A. (2024). Perlindungan Konsumen Sektor Keuangan: Peran OJK dalam Menghadapi Ancaman Phising dan Skimming. Iuris Studia: Jurnal Kajian Hukum, 5(2), 347–363.

Mairul, & Dewi, K. D. (2018). Pelaksanaan Penyelesaian Sengketa Konsumen Melalui Jalur non Litigasi. Pagaruyuang Law Journal, 1(2), 254–276.

Marlina, A., & Bimo, W. A. (2018). Digitalisasasi Bank Terhadap Peningkatan Pelayanan Dan Kepuasan Nasabah Bank. INOVATOR, 7(1), 14. https://doi.org/10.32832/inovator.v7i1.1458

Mewu, M. Y. S., & Mahadewi, K. J. (2023). Perlindungan Konsumen Dalam Pembelian Produk Online: Analisis Perspektif Hukum Perlindungan Konsumen di Indonesia. Jurnal Kewarganegaraan, 7(1), 441–450.

Ngamal, Y., & Perajaka, M. A. (2021). PENERAPAN MODEL MANAJEMEN RISIKO TEKNOLOGI DIGITAL DI LEMBAGA PERBANKAN BERKACA PADA CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN INDONESIA. JURNAL MANAJEMEN RISIKO, 2(2), 59–74. https://doi.org/10.33541/mr.v2iIV.4099

Pratama, A. P. R. (2021). Penguatan Digitalisasi Perbankan dalam Pelayanan Costumer Service Nasabah Secara Digital di Masa Covid-19. Simbur Cahaya, 28(2), 312. https://doi.org/10.28946/sc.v28i2.1443

Priambodo, A., Andriani, A., Yuniawati, R., Hamidin, D., Sulaeman, M., Dharmawan, A., Suhardi, & Martono, S. (2022). Transformasi Indonesia Menuju Cashless Society.

Purba, R. A., Sudarso, A., Silitonga, H. P., Sisca, Supitriyani, Yusmanizar, Nainggolan, L. E., Sudirman, A., Widyastuti, R. D., Novita, A. D., & Teri. (2020). Aplikasi Teknologi Informasi: Teori dan Implementasi. Penerbit Yayasan Kita Menulis.

Putri, D. C. P., & Lutfianti, A. (2024). Peran Teknologi Finansial FinTech dalam Mengubah Layanan Perbankan Tradisional. Media Hukum Indonesia (MHI), 2(4), 194–201.

Putri, D. F., Andriani, Sari, W. R., & Nabbila, F. L. (2023). ANALISIS PERLINDUNGAN NASABAH BSI TERHADAP KEBOCORAN DATA DALAM MENGGUNAKAN DIGITAL BANKING. JIEM : Jurnal Ilmiah Ekonomi Dan Manajemen, 1(4), 173–181.

Ramadhani, F. (2023). DINAMIKA UU ITE SEBAGAI HUKUM POSITIF DI INDONESIA GUNA MEMINIMALISIR KEJAHATAN SIBER. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora, 1(1), 89–97. https://doi.org/10.572349/kultura.v1i1.98

Risqiana, R., Hayfa, J., Rani, R., & Wungkana, S. R. (2024). Implementation of Data Protection Authority (DPA) in Indonesia: The Urgency of Legal Protection of Customer's Personal Data in E-Banking Service Transactions. Jurnal Penelitian Ilmu-Ilmu Sosial, 5(1), 19–33. https://doi.org/10.23917/sosial.v5i1.2375

Rizieq, M., & Suwarsit. (2024). Transformasi Layanan Perbankan dari Antrian Panjang Menuju Banking in Your Pocket. BanKu: Jurnal Perbankan Dan Keuangan, 5(2), 291–299.

Suryanto, D., Riyanto, S., & Arifudin. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Dalam Industri Ritel Tinjauan Terhadap Kepatuhan Dan Dampaknya Pada Konsumen. VERTAS, 10(1), 121–135.

Tarantang, J., Syawaliah, S., Astiti, N. N., & Kasenda, D. (2023). PERLINDUNGAN HUKUM NASABAH DALAM PENYELENGGARAN LAYANAN PERBANKAN DIGITAL. Belom Bahadat, 13(1), 21–40. https://doi.org/10.33363/bb.v13i1.949

Tarigan, H. A. A. B., & Paulus, D. H. (2019). PERLINDUNGAN HUKUM TERHADAP NASABAH ATAS

PENYELENGGARAAN LAYANAN PERBANKAN DIGITAL. Jurnal Pembangunan Hukum Indonesia, 1(3), 294–307. https://doi.org/10.14710/jphi.v1i3.294-307