Yurisprudentia: Jurnal Hukum Ekonomi
Vol. 10 No. 2 Desember 2024
E-ISSN: 2580-5234, P-ISSN: 2442-6822
Web: http://jurnal.iain-padangsidimpuan.ac.id/index.php/yurisprudentia

Perlindungan Hukum bagi Nasabah dalam Kasus Phising dan Siber Perbankan di Indonesia

Intania Az-zahra[1], Zaky Munthaha Labib, S.H., M.H.[2]

Universitas Islam Negeri Sunan Gunung Djati[1], Universitas Islam Negeri Sunan Gunung Djati[2]
E-Mail; intaniazara063@gmail.com [1] , munthahalabibzaky@gmail.com [2]

Abstrak

Penelitian ini membahas perlindungan hukum bagi nasabah bank dalam kasus penipuan perbankan digital, dengan fokus pada phishing dan kejahatan siber di Indonesia. Era digitalisasi yang pesat telah membawa kemudahan dan efisiensi dalam transaksi perbankan, tetapi juga memperkenalkan risiko signifikan, seperti kejahatan siber yang menargetkan data pribadi dan keamanan finansial. Penelitian ini menyoroti peran otoritas pengawas seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia dalam mengawasi dan membimbing sektor perbankan untuk meningkatkan keamanan digital. Penelitian ini juga mengkaji penerapan hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perbankan untuk menangani kejahatan phishing dan memastikan keadilan bagi nasabah yang terdampak. Temuan penelitian ini menekankan pentingnya kolaborasi antara bank, pemerintah, dan otoritas hukum dalam menerapkan langkah-langkah keamanan yang kuat, pendidikan konsumen, dan penegakan hukum untuk menciptakan ekosistem perbankan digital yang aman. Upaya meningkatkan keamanan siber, bersama dengan sanksi tegas bagi pelaku kejahatan siber, bertujuan untuk meminimalkan penipuan perbankan digital dan melindungi kepercayaan serta integritas data nasabah.

Kata kunci: Otoritas Jasa Keuangan, Bank Indonesia, pengawasan bank, pembinaan bank.

Abstract

This paper discusses legal protection for bank customers in cases of digital banking fraud, focusing on phishing and cybercrime in Indonesia. The rapid digitalization era has brought convenience and efficiency in banking transactions, but it has also introduced significant risks, such as cybercrimes targeting personal data and financial security. This research highlights the role of regulatory bodies like the Financial Services Authority (OJK) and Bank Indonesia in

supervising and guiding the banking sector to enhance digital security. It examines the application of laws such as the Electronic Information and Transactions Law (UU ITE) and the Banking Law to address phishing crimes and ensure justice for affected customers. The findings underscore the importance of collaboration between banks, government, and legal authorities in implementing robust security measures, consumer education, and law enforcement to create a safe digital banking ecosystem. Efforts to enhance cybersecurity, alongside strict penalties for cybercriminals, aim to minimize digital banking fraud and protect customers' trust and data integrity.

Keywords: Financial Services Authority, Bank Indonesia, bank supervision, bank guidance.

A. Pendahuluan

Di era modern dan digitalisasi saat ini, banyak sekali perubahan dalam kebiasaan masyarakat dan kebutuhan yang dialihkan dalam bentuk digital. Hampir seluruh aktivitas masyarakat menggunakan teknologi digital, seperti bekerja, belajar, berbelanja, hingga transaksi keuangan. Perbankan di Indonesia juga telah mengadopsi sistem Internet Banking untuk memudahkan nasabah dalam melakukan transaksi keuangan. Dengan kemampuan menembus batas waktu dan tempat, layanan Internet Banking memberikan fleksibilitas, efisiensi, dan kesederhanaan kepada pengguna.[1]

Namun, di balik kemudahan yang ditawarkan, muncul risiko yang signifikan, seperti pelanggaran hukum yang melibatkan data pribadi dan risiko keuangan yang dihadapi oleh nasabah bank. Kemajuan teknologi informasi tidak hanya membawa manfaat, tetapi juga peluang bagi para pelaku kejahatan untuk melakukan berbagai aktivitas kriminal. Fenomena ini dikenal sebagai kejahatan siber (*cybercrime*), yang melibatkan penggunaan komputer dan perangkat elektronik lainnya sebagai alat kejahatan. Salah satu bentuk kejahatan siber yang sering terjadi adalah phishing, yaitu

[1] S Putrianda, "Analisis Hukum Terhadap Perlindungan Nasabah Dalam Menggunakan Internet Banking Di Indonesia (Studi Kasus Bank X)," *"Dharmasisya" Jurnal Program Magister Hukum …* 2, no. January (2023).

penipuan yang bertujuan mencuri informasi pribadi nasabah.[2]

Kejahatan yang dilakukan dalam dunia internet semakin meningkat, mencakup berbagai modus seperti penipuan yang mengatasnamakan bank hingga manipulasi dalam prosedur transaksi jual beli. Salah satu kasus terbaru adalah pencurian data nasabah yang menyimpan uang di Bank Syariah Indonesia, yang merupakan bank milik pemerintah. Di sisi lain, penggunaan transaksi keuangan digital, meskipun menawarkan kemudahan dan efisiensi, juga berpotensi menimbulkan risiko serupa, seperti phising, kejahatan siber, dan kebocoran data pribadi. Perlindungan yang disediakan oleh sistem digital saja tidak cukup, mengingat semakin kompleksnya modus operandi pelaku kejahatan dengan keahlian yang mereka miliki. Oleh karena itu, diperlukan perlindungan hukum yang komprehensif bagi nasabah bank, khususnya dalam penggunaan layanan perbankan digital, guna memberikan rasa aman dan menjamin hak-hak mereka.[3]

Kejahatan siber yang melibatkan pencurian data nasabah sering kali diikuti oleh permintaan tebusan kepada pihak pemerintah sebagai upaya untuk mengembalikan dana nasabah yang hilang. Tidak jarang, saldo rekening nasabah mengalami kerugian signifikan hingga hilang tanpa meninggalkan jejak. Selain itu, data pribadi nasabah yang dicuri kerap disimpan oleh pelaku kejahatan siber untuk dimanfaatkan di masa mendatang. Kejahatan serupa juga terjadi pada BRI melalui salah satu layanan mereka, yaitu BRI Life, di mana data seluruh nasabah berhasil dicuri oleh pihak yang tidak bertanggung jawab.[4]

Kejahatan siber juga membawa dampak yang serius terhadap hukum ekonomi, termasuk hukum ekonomi syariah. Sistem perbankan syariah yang mengedepankan prinsip keadilan, transparansi, dan perlindungan terhadap nasabah menghadapi tantangan besar dalam menjaga integritasnya di tengah ancaman kejahatan digital. Ketidakjelasan tanggung jawab antara bank dan nasabah dalam kasus penipuan dan kebocoran data sering kali menghambat penyelesaian kasus secara adil. Akibatnya, banyak nasabah yang merasa kesulitan mendapatkan keadilan karena kurang memahami mekanisme hukum yang

[2] Delvyan Putri Surya Ningrum and Jamiatur Robekha, "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia," *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora* 2, no. 4 (2023): 765–76, https://doi.org/10.56799/peshum.v2i4.2115.
[3] Delvyan Putri Surya Ningrum and Jamiatur Robekha.
[4] Delvyan Putri Surya Ningrum and Jamiatur Robekha.

berlaku. Dalam menghadapi tantangan ini, diperlukan perlindungan hukum yang komprehensif dan proaktif. Bank memiliki tanggung jawab besar untuk terus meningkatkan keamanan sistem digital mereka, sementara pemerintah dan otoritas hukum perlu menetapkan regulasi yang tegas untuk menangani kejahatan siber. Pendidikan bagi masyarakat tentang bahaya phishing dan cara melindungi data pribadi juga menjadi langkah penting untuk menciptakan ekosistem perbankan digital yang aman.[5]

Oleh karena itu, Penelitian ini bertujuan untuk menganalisis perlindungan hukum yang berlaku di Indonesia bagi nasabah bank dalam menghadapi kasus penipuan digital, pencurian data pribadi, dan phishing. Diharapkan penelitian ini dapat memberikan kontribusi yang signifikan dalam memperkuat sistem hukum nasional agar lebih adaptif dan mampu menjawab berbagai tantangan yang muncul di era digital.

B. Metode Penelitian

Metode penelitian yang digunakan dalam artikel ini adalah studi kepustakaan (*library research*), yaitu pendekatan yang melibatkan pengumpulan dan analisis data dari berbagai literatur yang relevan untuk memperoleh pemahaman mendalam mengenai perlindungan hukum bagi nasabah bank di Indonesia dalam kasus penipuan digital, pencurian data pribadi, dan phishing. Penulis mengacu pada sumber yang kredibel seperti peraturan dari Otoritas Jasa Keuangan (OJK).

Pendekatan ini dilakukan melalui identifikasi, seleksi, dan analisis dokumen resmi, seperti regulasi hukum, laporan tahunan, kebijakan yang diterbitkan oleh OJK , serta studi kasus yang relevan. Selain itu, penulis juga menganalisis literatur akademik, jurnal hukum, dan laporan penelitian terkait kejahatan siber di sektor perbankan, untuk memastikan bahwa pembahasan didasarkan pada data dan analisis yang komprehensif. Pendekatan ini bertujuan untuk memberikan gambaran yang akurat dan mendalam mengenai tantangan serta peluang dalam meningkatkan perlindungan hukum bagi nasabah di era digital.

[5] Imelia Damai Agusthin, Dinda Christy Nada, and Nadia Ananda Putri, "Perlindungan Hukum Nasabah Dari Kejahatan Phising Dalam Layanan Perbankan Digital Di Indonesia," 2024, 132–48.

C. Pembahasan/ Hasil Penelitian

Perlindungan hukum merupakan mekanisme yang dirancang untuk melindungi hak asasi individu maupun kelompok dari tindakan yang melanggar hukum atau merugikan. Perlindungan ini dapat diberikan melalui peraturan perundang-undangan maupun langkah-langkah preventif dan represif oleh pemerintah. Tujuan utamanya adalah menjamin keadilan serta memberikan sanksi yang tegas kepada pihak-pihak yang melanggar hukum.[6]

Menurut Satjipto Rahardjo, perlindungan hukum memiliki peran penting dalam menjaga keseimbangan antara hak dan kewajiban, serta mencegah perilaku yang dapat mengganggu tatanan hukum yang berlaku. Selain memberikan perlindungan fisik, perlindungan hukum juga mencakup upaya melindungi kepentingan hukum seseorang agar mereka dapat menjalankan hak-haknya tanpa ancaman atau gangguan yang melawan hukum.[7]

Seiring dengan kemajuan digitalisasi, tantangan baru muncul, khususnya dalam sektor perbankan. Digitalisasi telah menjadi pendorong utama transformasi sektor perbankan dalam beberapa dekade terakhir. Teknologi informasi memungkinkan bank untuk memperluas jangkauan layanan mereka, memberikan kemudahan kepada nasabah dalam melakukan berbagai transaksi tanpa harus mengunjungi cabang fisik. Dari layanan transfer uang, pembayaran tagihan, hingga pengelolaan investasi, semuanya kini dapat diakses melalui perangkat digital seperti smartphone atau komputer. Transformasi ini membawa efisiensi dan kenyamanan, serta meningkatkan pengalaman pelanggan secara keseluruhan.[8]

Bagi bank, digitalisasi menawarkan manfaat besar dalam mengurangi biaya operasional melalui pengurangan kebutuhan layanan fisik dan dokumen cetak. Di sisi lain, nasabah mendapatkan akses yang lebih cepat, fleksibel, dan praktis ke berbagai layanan perbankan, kapan saja dan di mana saja. Fitur seperti mobile banking, internet banking, dan dompet digital telah mengubah cara orang berinteraksi dengan keuangan mereka, menjadikan aktivitas keuangan menjadi lebih mudah dan efisien. [9]

[6] A Setiawan, "Perlindungan Hukum Dalam Perspektif Hak Asasi Manusia.," *Jurnal Ilmu Hukum* 7, no. 2 (2015): 123–35.
[7] S Rahardjo, *Hukum Dalam Jagat Ketertiban* (Jakarta: Penerbit Huma, 2009).
[8] Agusthin, Nada, and Putri, hlm 135.
[9] Financial Services Authority. (2022). *Digital Banking Governance and Risk Management*. Jakarta: Financial Services Authority.

Namun, meskipun membawa banyak manfaat, digitalisasi juga memiliki sisi lain yang perlu diwaspadai. Keamanan dalam perbankan digital menjadi tantangan besar yang harus dihadapi. Salah satu ancaman yang paling sering terjadi adalah phishing, yaitu jenis penipuan di mana pelaku kejahatan berusaha mendapatkan informasi pribadi atau sensitif seperti kata sandi, nomor kartu kredit, atau identitas lainnya. Phishing sering dilakukan melalui email, situs web palsu, atau pesan yang tampak resmi, sehingga sulit dikenali oleh pengguna awam. Ancaman-ancaman semacam ini mencerminkan risiko serius yang perlu diantisipasi dalam ekosistem perbankan digital yang terus berkembang.

Meningkatnya ketergantungan pada teknologi dan data elektronik telah membuka peluang bagi terjadinya kejahatan siber, seperti phishing, di sektor perbankan digital. Ketika sistem digital menjadi bagian penting dalam transaksi keuangan, risiko kebocoran data pribadi juga meningkat. Phishing adalah bentuk kejahatan siber di mana pelaku memanfaatkan kelemahan sistem keamanan pengguna untuk mencuri data pribadi, termasuk kredensial akun dan nomor rekening. Hal ini sering terjadi melalui situs palsu, email manipulatif, atau pesan yang menyerupai institusi resmi.[10] Salah satu kasus phishing terjadi pada nasabah PT Bank Rakyat Indonesia (Persero) Tbk., di mana pelaku menggunakan situs palsu untuk mencuri data pribadi nasabah, yang mengakibatkan kerugian finansial serta penurunan kepercayaan terhadap layanan perbankan digital. Berdasarkan data Indonesia Anti-Phishing Data Exchange (IDADX), terdapat 23.675 kasus phishing di Indonesia sepanjang Januari–Maret 2023.

Bank digital memiliki tanggung jawab besar untuk melindungi sistem mereka dari ancaman ini. Regulasi seperti Peraturan Otoritas Jasa Keuangan (POJK) Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi mewajibkan bank digital untuk menjaga ketahanan siber dan menerapkan tata kelola teknologi informasi yang efektif. Pasal 2 dan Pasal 21 dalam peraturan tersebut menekankan pentingnya menyediakan layanan yang aman, andal, dan bertanggung jawab. Pelanggaran terhadap regulasi ini dapat menyebabkan sanksi administratif, mulai dari teguran hingga pembekuan kegiatan usaha tertentu, bahkan berdampak negatif pada reputasi dan kesehatan bank. [11]

[10] Agusthin, Nada, and Putri, hlm. 135-136.

[11] Agusthin, Nada, and Putri, hlm. 136.

Untuk menghadapi ancaman phishing, bank digital perlu mengadopsi langkah-langkah mitigasi yang komprehensif. Strategi utama meliputi penerapan teknologi keamanan mutakhir seperti enkripsi data, autentikasi dua faktor, dan sistem deteksi aktivitas mencurigakan. Selain itu, edukasi kepada nasabah juga sangat penting untuk membantu mereka mengenali dan menghindari ancaman phishing. Bank digital juga harus melakukan audit keamanan secara berkala untuk memastikan sistem tetap aman dan relevan dengan perkembangan teknologi. Lebih lanjut, kolaborasi dengan regulator dan otoritas terkait diperlukan untuk mengembangkan kebijakan yang efektif dalam menghadapi ancaman siber. Dengan penerapan teknologi keamanan yang canggih, transparansi dalam pengelolaan risiko, serta edukasi berkelanjutan kepada nasabah, bank digital dapat membangun kepercayaan masyarakat sekaligus menjaga stabilitas sektor perbankan di era digital.

Selain itu, POJK tentang Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan mengatur bahwa bank digital harus menerapkan prinsip perlindungan konsumen. Pasal 21 ayat (1) mewajibkan bank untuk menyediakan layanan pengaduan nasabah yang dapat diakses selama 24 jam, selain memastikan keamanan teknis yang memadai, bank digital juga bertanggung jawab untuk memberikan edukasi kepada nasabah, sehingga mereka mampu mengenali tanda-tanda phishing, seperti email atau situs web palsu yang mencoba mencuri informasi sensitif. [12]

Pasal 21 POJK juga menegaskan bahwa bank digital harus menerapkan manajemen risiko yang komprehensif. Ini berarti bahwa bank tidak hanya perlu memiliki langkah pencegahan, tetapi juga harus siap dengan protokol respons terhadap insiden keamanan. Dalam hal terjadi pelanggaran, bank wajib segera menginformasikan kepada pihak yang terkait, termasuk Otoritas Jasa Keuangan (OJK) dan nasabah yang terdampak. Tindakan ini bertujuan untuk meminimalkan dampak negatif dari insiden keamanan serta memulihkan kepercayaan publik.

Sanksi administratif yang diatur dalam POJK Nomor 11 Tahun 2022 menjadi pengingat penting bagi bank digital untuk serius dalam menjaga keamanan. Bank yang gagal memenuhi kewajiban ini dapat dikenai teguran tertulis, pembekuan kegiatan usaha tertentu, atau bahkan penurunan nilai

[12] Agusthin, Nada, and Putri, hlm. 136.

tata kelola. Sanksi ini tidak hanya berdampak pada reputasi bank, tetapi juga dapat memengaruhi kesehatan keuangan bank secara keseluruhan.

Keamanan siber yang buruk juga dapat memicu konsekuensi jangka panjang yang lebih luas. Kepercayaan publik terhadap sistem perbankan digital dapat menurun jika insiden pelanggaran data terjadi secara berulang. Oleh karena itu, bank digital harus terus meningkatkan kemampuan mereka dalam mengelola risiko siber. Investasi dalam teknologi keamanan, pelatihan untuk staf, dan pengembangan kebijakan internal yang ketat adalah langkah-langkah penting yang harus diambil. Selain itu, kolaborasi dengan regulator, lembaga keamanan siber, dan penyedia teknologi juga menjadi faktor penting dalam memperkuat sistem keamanan.

Tidak hanya itu, bank digital perlu mengadopsi pendekatan proaktif dengan melakukan simulasi ancaman siber secara berkala. Langkah ini bertujuan untuk menguji ketahanan sistem terhadap serangan dan memastikan bahwa protokol respons insiden berjalan dengan efektif. Dengan demikian, potensi kerugian dapat diminimalkan dan sistem dapat terus diperbaiki untuk menghadapi ancaman yang berkembang.

Pada akhirnya, tanggung jawab bank digital dalam menjaga keamanan sistem mereka bukan hanya untuk melindungi nasabah, tetapi juga untuk menjaga stabilitas industri perbankan secara keseluruhan. Dalam dunia yang semakin terhubung, keamanan siber bukan lagi pilihan, melainkan keharusan. Dengan mematuhi regulasi yang ada dan berkomitmen untuk terus berinovasi, bank digital dapat menjadi pelopor dalam menciptakan ekosistem perbankan yang aman, andal, dan berkelanjutan.

Tanggung jawab perlindungan konsumen ini juga mencakup memastikan transparansi dalam setiap layanan yang ditawarkan. Bank digital wajib memberikan informasi yang jelas dan mudah dipahami terkait biaya, risiko, dan ketentuan yang berlaku pada produk atau layanan mereka. Ini penting untuk menghindari kesalahpahaman yang dapat menyebabkan ketidakpuasan atau konflik di kemudian hari. Informasi yang transparan juga meningkatkan kepercayaan nasabah terhadap bank digital sebagai lembaga yang mengutamakan kepentingan konsumen.

Dalam menangani pengaduan, bank digital harus memiliki sistem yang responsif dan efisien. Layanan pelanggan 24 jam yang disebutkan dalam regulasi memungkinkan nasabah untuk melaporkan masalah kapan saja.

Proses penanganan pengaduan harus dilakukan dengan cepat dan profesional, termasuk memberikan solusi yang memadai jika masalah tersebut disebabkan oleh kegagalan sistem atau kelalaian bank. Mekanisme pengaduan yang baik adalah salah satu indikator bahwa bank menghargai nasabahnya dan berkomitmen untuk memberikan layanan terbaik.

Tidak kalah penting, bank digital juga harus mengembangkan langkah-langkah pencegahan untuk meminimalkan risiko yang dapat merugikan nasabah. Ini mencakup implementasi teknologi keamanan mutakhir, seperti enkripsi data, autentikasi multi-faktor, dan pemantauan aktivitas mencurigakan. Selain itu, bank perlu bekerja sama dengan regulator dan lembaga keamanan siber untuk terus memperbarui protokol perlindungan konsumen sesuai dengan perkembangan ancaman yang ada.

Bank digital juga memiliki tanggung jawab sosial untuk mendukung literasi keuangan masyarakat luas, termasuk mereka yang belum menjadi nasabah. Dengan menyediakan materi edukasi umum tentang pengelolaan keuangan, investasi, dan manajemen risiko, bank dapat membantu meningkatkan kesejahteraan masyarakat sekaligus memperkuat posisinya sebagai lembaga yang berorientasi pada konsumen.

Secara keseluruhan, tanggung jawab bank digital dalam melindungi konsumen mencerminkan peran mereka sebagai pilar penting dalam ekosistem keuangan modern. Dengan mematuhi regulasi yang ada dan mengambil langkah-langkah proaktif untuk melindungi serta mengedukasi nasabah, bank digital dapat menciptakan lingkungan perbankan yang lebih inklusif, aman, dan berkelanjutan. Tanggung jawab ini tidak hanya berdampak positif bagi nasabah, tetapi juga memperkuat posisi bank sebagai institusi yang dipercaya oleh masyarakat.[13]

Menurut POJK Nomor 3 Tahun 2023 tentang Peningkatan Literasi dan Inklusi Keuangan, bank digital harus menerapkan program edukasi dalam rencana tahunan mereka untuk meningkatkan pemahaman pelanggan tentang produk dan layanan perbankan digital. Salah satu bentuk pendidikan ini adalah sosialisasi, yaitu bekerja sama dengan organisasi pemerintah, akademisi, organisasi non pemerintah, atau pihak lain yang memiliki tujuan

[13] Anshori, M. (2021). *Etika dan Teknologi Informasi dalam Dunia Perbankan*. Malang: Universitas Negeri Malang Press.

yang sama. Bank digital melakukan langkah-langkah ini untuk memperkuat sistem keamanan mereka dan meningkatkan kesadaran masyarakat terhadap risiko dan perlindungan yang terkait dengan layanan perbankan digital.[14]

Salah satu bentuk pendidikan yang dimandatkan adalah sosialisasi, di mana bank digital bekerja sama dengan berbagai pihak seperti organisasi pemerintah, akademisi, organisasi non pemerintah (NGO), atau lembaga lain yang memiliki visi serupa. Kerja sama ini memungkinkan bank untuk menjangkau segmen masyarakat yang lebih luas dan memberikan informasi yang relevan dan mudah dipahami oleh berbagai kelompok, termasuk mereka yang belum sepenuhnya terpapar teknologi digital atau layanan keuangan formal.

Program sosialisasi ini dapat dilakukan melalui seminar, lokakarya, pelatihan, atau kampanye edukasi yang menggunakan media digital maupun offline. Materi yang disampaikan mencakup berbagai aspek, mulai dari cara menggunakan layanan perbankan digital secara aman, mengenali ancaman seperti phishing, mengenali tanda-tanda phishing, dan menghindari penipuan lainnya hingga memahami manfaat dan risiko dari produk perbankan tertentu. Dengan cara ini, masyarakat menjadi lebih waspada terhadap risiko yang terkait dengan penggunaan layanan perbankan digital. Dengan pendekatan yang informatif dan praktis, masyarakat dapat lebih mudah mengadopsi layanan perbankan digital dengan keyakinan yang lebih besar terhadap keamanannya.[15]

Langkah-langkah edukasi ini tidak hanya bertujuan untuk meningkatkan literasi keuangan masyarakat, tetapi juga berfungsi sebagai upaya pencegahan untuk memperkuat sistem keamanan bank digital. Ketika nasabah memahami cara melindungi data pribadi dan mengenali potensi ancaman siber, mereka secara tidak langsung membantu mengurangi risiko pelanggaran keamanan yang dapat berdampak negatif pada mereka maupun bank itu sendiri. Ini menciptakan situasi win-win di mana nasabah dan bank sama-sama diuntungkan.[16]

Selain itu, bank digital juga memiliki tanggung jawab untuk

[14] S Chairunnisa, T Murwadji, and N Harrieti, "Perlindungan Hukum Terhadap Nasabah Atas Kejahatan Phising Dan Hacking Pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia.," *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 1 (2024): 01–16.

[15] Kementerian Komunikasi dan Informatika. (2023). *Pedoman Keamanan Informasi untuk Perbankan Digital. **Jakarta: Kominfo.***

[16] Setyawan, D. (2021). "Cybersecurity in Digital Banking: A Case Study in Indonesia." *International Journal of Banking Technology*, 12(4), 389–402.

menyediakan materi edukasi yang menarik dan mudah diakses, seperti video tutorial, panduan langkah demi langkah, atau simulasi interaktif yang dapat diakses melalui aplikasi atau situs web mereka. Dengan memanfaatkan teknologi, bank dapat menjangkau audiens yang lebih luas, termasuk generasi muda yang lebih akrab dengan media digital, serta membantu mereka mengembangkan kebiasaan keuangan yang sehat sejak dini.[17]

Melalui edukasi ini, bank digital juga berkontribusi dalam mendorong inklusi keuangan, terutama bagi kelompok masyarakat yang selama ini kurang terlayani oleh lembaga keuangan tradisional. Dengan memberikan pengetahuan yang memadai, masyarakat yang sebelumnya tidak memiliki akses atau pemahaman tentang layanan keuangan dapat mulai terlibat dalam ekosistem perbankan digital, sehingga membantu mereka mencapai kemandirian finansial.

Kerja sama dengan akademisi dan organisasi lain juga memungkinkan bank digital untuk memahami kebutuhan masyarakat secara lebih mendalam. Data dan wawasan yang diperoleh melalui kolaborasi ini dapat digunakan untuk merancang program edukasi yang lebih relevan dan berdampak. Misalnya, bank dapat mengidentifikasi kelompok masyarakat tertentu yang membutuhkan perhatian khusus, seperti pelaku usaha kecil, petani, atau ibu rumah tangga, dan menyusun materi yang sesuai dengan kebutuhan mereka.

Edukasi yang terencana dengan baik juga membantu meningkatkan kepercayaan masyarakat terhadap layanan perbankan digital. Nasabah yang merasa dilindungi dan dihargai oleh bank cenderung memiliki loyalitas yang lebih tinggi, sehingga memperkuat hubungan jangka panjang antara bank dan pelanggan. Hal ini tidak hanya meningkatkan reputasi bank, tetapi juga memperluas basis pengguna layanan mereka.[18]

Dalam konteks ini, regulasi POJK Nomor 3 Tahun 2023 mencerminkan pentingnya peran bank digital dalam menciptakan ekosistem keuangan yang aman, inklusif, dan berkelanjutan. Dengan menerapkan program edukasi secara konsisten, bank digital tidak hanya memenuhi kewajiban regulasi, tetapi juga berkontribusi pada pemberdayaan masyarakat dan

[17] Prasetyo, T. A., & Hidayat, R. (2021). "Digital Banking in Indonesia: Opportunities and Challenges." *Journal of Financial Innovation and Technology*, 15(3), 250–270.

[18] Suryanto, D. (2022). *Keamanan Data dalam Era Digitalisasi Perbankan*. Yogyakarta: Gadjah Mada University Press.

pembangunan ekonomi yang lebih luas. Program ini menjadi langkah strategis yang membawa manfaat jangka panjang, baik bagi bank maupun masyarakat sebagai pengguna layanan.

Dengan meningkatkan literasi keuangan, masyarakat tidak hanya menjadi lebih percaya diri dalam menggunakan layanan keuangan, tetapi juga memiliki peluang lebih besar untuk meningkatkan kesejahteraan mereka melalui pengelolaan keuangan yang lebih baik. Hal ini selaras dengan tujuan inklusi keuangan untuk menjangkau seluruh lapisan masyarakat, termasuk kelompok yang selama ini belum sepenuhnya terlibat dalam ekosistem keuangan formal.[19]

Kerja sama antara bank digital dan berbagai pihak juga berkontribusi pada pengembangan kebijakan yang lebih efektif dalam meningkatkan literasi keuangan.[20] Melalui kolaborasi dengan akademisi dan organisasi lainnya, bank dapat memperoleh masukan berharga tentang kebutuhan masyarakat dan tantangan yang mereka hadapi. Data dan wawasan ini kemudian dapat digunakan untuk merancang program edukasi yang lebih relevan dan berdampak.[21]

Selain itu, upaya edukasi ini juga membantu memperkuat reputasi bank digital sebagai lembaga yang peduli terhadap kebutuhan masyarakat. Bank yang aktif dalam meningkatkan literasi keuangan cenderung mendapatkan kepercayaan lebih besar dari nasabah, yang pada akhirnya dapat meningkatkan loyalitas pelanggan dan memperluas basis pengguna mereka. Dalam jangka panjang, hal ini tidak hanya menguntungkan bank, tetapi juga memperkuat ekosistem perbankan digital secara keseluruhan. Pada akhirnya, penerapan program edukasi seperti yang diwajibkan dalam POJK Nomor 3 Tahun 2023 merupakan langkah strategis untuk menciptakan ekosistem perbankan digital yang inklusif, aman, dan berkelanjutan. Dengan meningkatkan kesadaran masyarakat tentang risiko dan perlindungan yang terkait dengan layanan perbankan digital, bank dapat memastikan bahwa transformasi digital di sektor keuangan berjalan dengan lancar dan memberikan manfaat maksimal bagi semua pihak yang terlibat.[22]

Pelaku phising tidak hanya

[19] Oktaviani, R. (2023). *Phishing dan Keamanan Data Perbankan: Strategi Pencegahan*. Surabaya: Universitas Airlangga Press.
[20] Bank Indonesia. (2021). **Statistik Sistem Pembayaran dan Perbankan Digital di Indonesia**. Jakarta: Bank Indonesia.
[21] Ghozali, I., & Chariri, A. (2020**).** *Teori Akuntansi: Konsep dan Implementasi***.** Semarang: Badan Penerbit Universitas Diponegoro
[22] Nasution, S. (2020**).** *Hukum dan Regulasi Perbankan di Indonesia***.** Bandung: Refika Aditama.

memanipulasi situs web atau surel untuk menyesatkan korban, tetapi mereka juga menggunakan kebohongan untuk menipu korban, yang pada akhirnya mengakibatkan kerugian bagi korban. Mengingat karakteristik kejahatan phishing dalam sistem perbankan digital yang melibatkan manipulasi dan penyalahgunaan sistem elektronik, berbagai ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dapat digunakan untuk menganalisis jenis kejahatan ini. Pasal 28 ayat (1) UU ITE melarang penyebaran atau transmisi informasi elektronik yang mengandung pemberitahuan atau informasi palsu yang menyebabkan kerugian material bagi konsumen selama transaksi elektronik. Menurut Pasal 45A ayat (1), pelanggaran ini dipidana dengan ancaman pidana penjara hingga enam tahun atau denda hingga satu miliar rupiah. Pelaku phishing biasanya mengirimkan email atau pesan elektronik yang menyesatkan dengan berpura-pura menjadi lembaga resmi untuk mengelabui korban untuk memberikan data sensitif seperti kredensial akun bank.[23]

Jika seseorang melakukan manipulasi informasi elektronik untuk membuat data yang digunakan tampak asli, pelaku dapat dikenakan Pasal 35 jo. Pasal 51 UU ITE, dengan ancaman 12 tahun penjara atau denda maksimal 12 miliar rupiah. Ini menunjukkan tingkat pelanggaran yang signifikan karena mengancam kepercayaan sistem elektronik. Selain itu, pelanggaran phishing dapat dijerat oleh Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE, yang menetapkan ancaman pidana maksimal delapan tahun penjara dan/atau denda hingga 800 juta untuk pelanggaran yang melanggar sistem keamanan elektronik. Lebih lanjut, Pasal 32 ayat 2 jo. Pasal 48 ayat 2 dapat menjerat pelaku yang memindahkan atau mengirimkan informasi elektronik, seperti mentransfer isi rekening korban ke akun lain tanpa izin. Ini adalah jenis phishing yang lebih kompleks yang bertujuan untuk memanfaatkan data korban secara ilegal. Untuk tindakan ini, ancaman pidana sembilan tahun penjara dan/atau denda maksimal tiga miliar.[24]

Kitab Undang-Undang Hukum Pidana (KUHP) menerapkan interpretasi ketat untuk kriminalisasi tindakan phishing fraud. Metode ini memungkinkan penerapan pasal-pasal

[23] Agusthin, Nada, and Putri, "Perlindungan Hukum Nasabah Dari Kejahatan Phising Dalam Layanan Perbankan Digital Di Indonesia."
[24] Aura Nasha Ramadhanti et al., "Cara Operasi Kejahatan Phising Di Ranah Siber Yang Diatur Oleh Positif Indonesia," *Jurnal Pendidikan Tambusai* 8, no. 1 (2024): 1299–1305.

dalam KUHP yang tidak secara eksplisit mengatur kejahatan berbasis elektronik dengan menemukan kesamaan unsur atau karakteristik tindak pidana tersebut. Sebagai contoh, phishing yang melibatkan pencurian data kartu kredit dapat dianggap sebagai tindak pidana pencurian menurut Pasal 362 KUHP. Selain itu, phishing yang dilakukan dengan membuat situs web palsu untuk menipu korban juga dapat dianggap sebagai tindak pidana penipuan menurut Pasal 378 KUHP, yang mengatur memanfaatkan tipu muslihat untuk memperoleh keuntungan secara tidak sah. Phishing fraud sering kali melibatkan lebih dari satu pelaku. Tindak pidana ini biasanya dilakukan secara terorganisir, di mana beberapa orang bekerja sama untuk melakukannya. Selain itu, Pasal 55 KUHP tentang keterlibatan dapat digunakan untuk menjerat semua pihak yang terlibat dalam pencurian, baik mereka yang secara langsung melakukan, membantu, atau memiliki peran lain yang mendukung pelaksanaan kejahatan tersebut. Dalam hal ini, KUHP juga menerapkan Pasal 363 ayat (4), yang memberikan pemberatan hukuman jika pencurian dilakukan oleh dua orang atau lebih secara bersama-sama.[25]

Selanjutnya, pasal 263 KUHP menetapkan sanksi hukum untuk tindak pidana pemalsuan surat, jika pelaku memalsukan atau membuat surat palsu yang seolah-olah asli dan dapat digunakan untuk menimbulkan hak, kewajiban, atau pembebasan utang. Selain itu, artikel ini membahas penggunaan surat palsu tersebut untuk menipu orang lain, terutama jika hal itu mengakibatkan kerugian bagi pihak tertentu. Pemalsuan surat dianggap sebagai kejahatan serius yang merusak kepercayaan dalam hubungan hukum dan sosial, dan hukuman untuk tindak pidana ini adalah penjara maksimal enam tahun. Ketika pelaku berusaha untuk menipu korban dengan membuat dokumen elektronik palsu, seperti email yang terlihat seperti komunikasi resmi dari bank atau lembaga tertentu, Pasal 263 KUHP dapat diterapkan. Dokumen elektronik palsu ini dapat berisi informasi pribadi seperti nomor rekening atau kata sandi yang mengarahkan korban untuk diberikan. Pelaku kemudian dapat menggunakan informasi ini untuk mendapatkan keuntungan pribadi. Pemalsuan dokumen fisik atau elektronik memiliki efek yang sama—mengakibatkan kerugian bagi korban dan mengganggu

[25] Agusthin, Nada, and Putri, "Perlindungan Hukum Nasabah Dari Kejahatan Phising Dalam Layanan Perbankan Digital Di Indonesia."

kepercayaan terhadap sistem administrasi, baik di tingkat institusional maupun pribadi. Oleh karena itu, artikel ini relevan. Oleh karena itu, membuat dan menggunakan dokumen elektronik palsu dapat dijerat dengan Pasal 263 KUHP, bersama dengan ketentuan dalam UU ITE. Penegak hukum dapat memberikan sanksi yang lebih keras dan memastikan bahwa pelaku phishing bertanggung jawab atas seluruh tindakannya.[26]

Kejahatan penipuan phishing yang sering menargetkan lembaga perbankan termasuk pencurian data melalui layanan perbankan online, mobile, dan informasi nomor kartu kredit. Karena akses ke data pelanggan dapat menghasilkan keuntungan finansial yang besar, bank menjadi sasaran utama pelaku phishing. Dalam menghadapi ancaman ini, hukum Indonesia mewajibkan bank untuk menjaga data pelanggan.[27]

Pasal 29 ayat (4) Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, yang telah diubah menjadi Undang-Undang Nomor 10 Tahun 1998, mengandung ketentuan yang sangat penting. Pasal ini mewajibkan bank untuk memberikan informasi kepada nasabah mengenai potensi risiko kerugian yang dapat timbul akibat transaksi yang dilakukan melalui bank. Tujuan dari ketentuan ini adalah untuk melindungi kepentingan nasabah dan memastikan bahwa mereka memahami risiko yang mungkin terjadi, terutama karena hubungan antara bank dan nasabah didasarkan pada kepercayaan.[28]

Pasal 40 ayat (1) dan (2) dari undang-undang yang sama juga mengatur perlindungan data pelanggan. Ayat-ayat ini mewajibkan bank untuk menjaga kerahasiaan data pelanggan, termasuk data yang disimpan dan disimpan. Bank memiliki tanggung jawab untuk mengelola dana masyarakat, jadi penting untuk menjaga privasi nasabah. Bank berharap dengan adanya ketentuan ini dapat menjaga kepercayaan terhadap sistem perbankan dengan menghindari penyalahgunaan atau akses ke data pelanggan.[29]

Selain itu, pihak bank juga dapat menerapkan prinsip-prinsip hukum ekonomi syariah seperti keadilan (‘adl), keseimbangan (tawazun), dan amanah (kepercayaan). Prinsip keadilan dapat

[26] Rhesita Yustitiana, “Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian Dari Upaya Penegakan Hukum Di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum,” *Jurnal Hukum Visio Justisia* 1, no. 1 (2021): 98–126.
[27] Agusthin, Nada, and Putri, “Perlindungan Hukum Nasabah Dari Kejahatan Phising Dalam Layanan Perbankan Digital Di Indonesia.”
[28] Agusthin, Nada, and Putri.
[29] Annisa Halimatu Sholihah, Kata Kunci, and Uang Palsu, “Tinjauan Hukum Terhadap Pertanggungjawaban Bank Kepada Data Nasabah Dalam Serangan Phishing,” *Indonesian Journal of Law* 1, no. 6 (2024): 186–94.

diwujudkan melalui transparansi dalam pengungkapan risiko kepada nasabah, serta mekanisme penyelesaian sengketa yang adil. Amanah, sebagai pilar utama dalam perbankan syariah, menuntut bank untuk menjaga kerahasiaan dan keamanan data nasabah dengan memanfaatkan teknologi canggih seperti enkripsi data dan autentikasi biometrik. Prinsip keseimbangan mendorong bank untuk menyesuaikan investasi dalam sistem keamanan digital dengan kebutuhan efisiensi layanan, sehingga tidak mengorbankan kenyamanan nasabah. Melalui kolaborasi dengan regulator dan otoritas hukum, bank syariah juga dapat berperan dalam mendukung pengembangan regulasi yang lebih kuat untuk memastikan perlindungan menyeluruh bagi nasabah di era digital. Dengan langkah-langkah ini, digitalisasi perbankan dapat terus memberikan manfaat maksimal, tanpa mengesampingkan aspek keamanan yang menjadi fondasi utama kepercayaan nasabah. Upaya perlindungan ini tidak hanya menjaga kepentingan nasabah tetapi juga memperkuat stabilitas dan reputasi sektor perbankan secara keseluruhan.

D. Kesimpulan dan Rekomendasi

POJK Nomor 3 Tahun 2023 tentang Peningkatan Literasi dan Inklusi Keuangan menekankan pentingnya peran bank digital dalam memberikan edukasi kepada masyarakat. Program edukasi ini dirancang untuk meningkatkan literasi keuangan masyarakat, sehingga mereka tidak hanya memahami cara menggunakan produk dan layanan perbankan digital, tetapi juga mampu mengenali dan mengelola risiko yang terkait dengan penggunaannya. Dengan pendekatan ini, bank digital dapat menciptakan hubungan yang lebih erat dan saling menguntungkan antara mereka dan nasabah. Edukasi menjadi komponen strategis dalam memastikan transformasi digital sektor perbankan berjalan secara inklusif dan berkelanjutan. Melalui sosialisasi dan kerja sama dengan berbagai pihak, seperti pemerintah, akademisi, dan NGO, bank digital dapat menjangkau segmen masyarakat yang lebih luas, termasuk kelompok yang sebelumnya kurang terlayani. Inisiatif ini juga membantu mempercepat pencapaian inklusi keuangan, terutama di wilayah yang memiliki akses terbatas terhadap layanan keuangan tradisional.

Salah satu fokus utama program edukasi ini adalah meningkatkan kesadaran masyarakat terhadap risiko

yang melekat pada layanan perbankan digital. Dengan memberikan informasi yang jelas dan praktis, masyarakat dapat lebih waspada terhadap ancaman seperti phishing dan penipuan online. Ini tidak hanya melindungi nasabah secara individu tetapi juga memperkuat sistem keamanan bank secara keseluruhan. Ketika nasabah menjadi lebih sadar dan teredukasi, risiko pelanggaran keamanan akibat kelalaian dapat diminimalkan. Bank digital juga diwajibkan untuk menyediakan materi edukasi yang mudah diakses, menarik, dan relevan dengan kebutuhan masyarakat. Dengan memanfaatkan teknologi digital, bank dapat menyebarluaskan informasi melalui platform seperti aplikasi, situs web, atau media sosial. Inovasi ini memungkinkan bank untuk menjangkau berbagai demografi, termasuk generasi muda yang cenderung lebih akrab dengan teknologi, sekaligus membantu mereka mengembangkan kebiasaan keuangan yang sehat.

Melalui program-program ini, bank digital juga dapat memperkuat reputasi mereka sebagai lembaga yang peduli terhadap kesejahteraan nasabah. Edukasi yang efektif meningkatkan kepercayaan masyarakat terhadap layanan perbankan digital, sehingga mendorong loyalitas nasabah. Dalam jangka panjang, kepercayaan ini menjadi aset berharga bagi bank dalam mempertahankan dan memperluas pangsa pasar mereka. Selain itu, kerja sama dengan pihak eksternal, seperti akademisi dan organisasi lain, memungkinkan bank digital untuk memperoleh wawasan yang lebih dalam tentang kebutuhan dan tantangan yang dihadapi masyarakat. Hal ini memberikan peluang bagi bank untuk merancang program edukasi yang lebih tepat sasaran dan relevan, sehingga dampaknya lebih signifikan. Dengan demikian, bank digital tidak hanya menjadi penyedia layanan keuangan, tetapi juga mitra yang aktif dalam pemberdayaan masyarakat.

Upaya peningkatan literasi keuangan juga berkontribusi pada penguatan inklusi keuangan. Dengan membantu masyarakat yang sebelumnya belum terjangkau oleh layanan keuangan formal untuk memahami manfaat dan cara menggunakan layanan perbankan digital, bank digital mendorong pertumbuhan ekonomi yang lebih inklusif. Ini sejalan dengan tujuan nasional untuk menciptakan akses keuangan yang lebih merata di seluruh lapisan masyarakat. Regulasi ini juga mendorong bank digital untuk mengambil peran aktif dalam menciptakan ekosistem perbankan yang

lebih aman. Edukasi yang diberikan kepada masyarakat secara tidak langsung mendukung upaya pencegahan risiko keamanan, seperti ancaman siber. Ketika masyarakat lebih teredukasi, ancaman terhadap data pribadi dan keamanan transaksi dapat ditekan, yang pada akhirnya mengurangi potensi kerugian bagi nasabah dan bank itu sendiri.

Pada akhirnya, program edukasi yang diwajibkan oleh POJK Nomor 3 Tahun 2023 tidak hanya berfungsi sebagai langkah pemenuhan regulasi, tetapi juga sebagai investasi jangka panjang bagi bank digital. Dengan menciptakan masyarakat yang lebih teredukasi dan inklusif dalam menggunakan layanan keuangan, bank digital memperkuat peran mereka dalam pembangunan ekonomi yang lebih luas. Inisiatif ini menciptakan ekosistem yang saling mendukung antara bank, nasabah, dan masyarakat. Kesimpulannya, peran edukasi yang diemban bank digital mencerminkan tanggung jawab mereka sebagai pelaku utama dalam transformasi keuangan digital. Dengan mematuhi regulasi dan melaksanakan program edukasi secara konsisten, bank digital dapat menciptakan lingkungan keuangan yang aman, inklusif, dan berkelanjutan. Hal ini tidak hanya memperkuat posisi mereka di pasar, tetapi juga mendukung tujuan nasional untuk meningkatkan literasi dan inklusi keuangan di Indonesia.

selanjutnya, berdasarkan analisis mengenai prinsip-prinsip yang harus diterapkan oleh bank digital untuk memastikan perlindungan hukum bagi nasabah, berikut adalah beberapa rekomendasi yang perlu diperhatikan: Pertama, prinsip keadilan ('*Adl*) mengharuskan bank untuk memastikan bahwa produk dan layanan yang ditawarkan adil dan tidak merugikan nasabah. Hal ini meliputi pemberian informasi yang jelas mengenai biaya, risiko, dan ketentuan layanan agar nasabah dapat membuat keputusan yang tepat. Selain itu, prinsip keseimbangan (*Tawazun*) mengingatkan bank untuk mempertimbangkan keseimbangan antara keuntungan yang diperoleh dan risiko yang dihadapi nasabah. Dengan demikian, bank perlu menghindari praktik yang dapat menimbulkan kerugian yang tidak proporsional bagi nasabah, dan memastikan bahwa layanan yang diberikan tidak hanya menguntungkan bank, tetapi juga bermanfaat bagi nasabah. Prinsip amanah (kepercayaan) juga menjadi aspek yang tak kalah penting, di mana bank harus menjaga kerahasiaan dan keamanan data nasabah. Penerapan teknologi keamanan yang mutakhir,

seperti enkripsi dan autentikasi multi-faktor, sangat diperlukan untuk memenuhi amanah tersebut. Selain itu, bank harus memiliki sistem yang responsif dalam menangani pengaduan dan masalah yang dihadapi nasabah. Dalam rangka meningkatkan literasi keuangan, bank perlu menjalankan program edukasi yang berkelanjutan agar nasabah lebih memahami produk dan layanan perbankan digital yang mereka gunakan. Dengan demikian, nasabah dapat membuat keputusan yang lebih bijak dan merasa lebih aman. Terakhir, kerjasama antara bank, Otoritas Jasa Keuangan (OJK), dan lembaga terkait lainnya sangat diperlukan untuk mengembangkan regulasi yang lebih ketat dan efektif guna melindungi nasabah. Hal ini mencakup pengawasan terhadap praktik perbankan digital serta penegakan hukum yang tegas terhadap kejahatan siber.

Referensi

Agusthin, Imelia Damai, Dinda Christy Nada, and Nadia Ananda Putri. "Perlindungan Hukum Nasabah Dari Kejahatan Phising Dalam Layanan Perbankan Digital Di Indonesia," 2024, 132–48.

Anshori, M. (2021). *Etika dan Teknologi Informasi dalam Dunia Perbankan***.** Malang: Universitas Negeri Malang Press.

Bank Indonesia. (2021). *Statistik Sistem Pembayaran dan Perbankan Digital di Indonesia*. Jakarta: Bank Indonesia.

Bank Indonesia. (2023). *POJK Nomor 3 Tahun 2023 tentang Peningkatan Literasi dan Inklusi Keuangan***.** Jakarta: Bank Indonesia.

Chairunnisa, S, T Murwadji, and N Harrieti. "Perlindungan Hukum Terhadap Nasabah Atas Kejahatan Phising Dan Hacking Pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia." *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 1 (2024): 01–16.

Delvyan Putri Surya Ningrum, and Jamiatur Robekha. "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia." *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora* 2, no. 4 (2023): 765–76. https://doi.org/10.56799/peshum.v2i4.2115.

*Financial Services Authority. (2022). Digital Banking Governance and Risk Management***.** Jakarta: Financial Services Authority.

Ghozali, I., & Chariri, A. (2020). *Teori Akuntansi: Konsep dan Implementasi***.** Semarang:

Badan Penerbit Universitas Diponegoro.

Halimatu Sholihah, Annisa, Kata Kunci, and Uang Palsu. "Tinjauan Hukum Terhadap Pertanggungjawaban Bank Kepada Data Nasabah Dalam Serangan Phishing." *Indonesian Journal of Law* 1, no. 6 (2024): 186–94. www.hukumonline.com.

Kementerian Komunikasi dan Informatika. (2023**).** *Pedoman Keamanan Informasi untuk Perbankan Digital*. Jakarta: Kominfo.

Nasution, S. (2020). *Hukum dan Regulasi Perbankan di Indonesia***.** Bandung: Refika Aditama.

Oktaviani, R. (2023). *Phishing dan Keamanan Data Perbankan: Strategi Pencegahan***.** Surabaya: Universitas Airlangga Press.

Otoritas Jasa Keuangan. (2023**).** *Laporan Tahunan Otoritas Jasa Keuangan 2023***.** Jakarta: Otoritas Jasa Keuangan.

Prasetyo, T. A., & Hidayat, R. (2021). "*Digital Banking in Indonesia: Opportunities and Challenges*." Journal of Financial Innovation and Technology, *15(3), 250–270.*

Putrianda, S. "Analisis Hukum Terhadap Perlindungan Nasabah Dalam Menggunakan Internet Banking Di Indonesia (Studi Kasus Bank X)." *"Dharmasisya" Jurnal Program Magister Hukum* 2, no. January (2023).

Rahayu, S., & Santoso, D. (2022). "*Peran Literasi Keuangan dalam Meningkatkan Inklusi Keuangan di Indonesia."* Jurnal Ekonomi dan Bisnis Indonesia, *10(2),* 120–140.

Rahardjo, S. *Hukum Dalam Jagat Ketertiban*. Jakarta: Penerbit Huma, 2009.

Ramadhanti, Aura Nasha, Tessa Ayuning Tias, Erin Dwi Lestari, and Asmak UI Hosnah. "Cara Operasi Kejahatan Phising Di Ranah Siber Yang Diatur Oleh Positif Indonesia." Jurnal Pendidikan Tambusai 8, no. 1 (2024): 1299–1305.

Rasyid, Arbanur, and Sawaluddin Siregar. "Fenomena Menarik Perkawinan Dibawah Umur Menjadi Trend Masa Kini Di Bittuju Tapanuli Selatan." *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam* 4, no. 1 (2022): 61–68. https://doi.org/10.37680/almanhaj.v4i1.1571.

Riyani, Irma. "Menelusuri Latar Historis Turunnya Alquran Dan Proses Pembentukan Tatanan Masyarakat Islam." *Al-Bayan: Jurnal Studi Ilmu Al- Qur'an Dan Tafsir* 1, no. 1 (2016): 27–34. https://doi.org/10.15575/al-bayan.v1i1.873.

Setiawan, A. "Perlindungan Hukum Dalam Perspektif Hak Asasi Manusia." Jurnal Ilmu Hukum 7, no. 2 (2015): 123–35.

Setyawan, D. (2021). "Cybersecurity in Digital Banking: A Case Study in Indonesia." *International Journal of Banking Technology*, 12(4), 389–402.

Siregar, Sawaluddin, and Misbah Mardiah. "Relevansi Term Kafa'ah Pada Pernikahan Adat Batak Mandailing Natal." *Jurnal Al-Maqasid; Jurnal Ilmu-Ilmu Kesyariahan Dan Keperdataan* 7 (2021): 290–302.

Suryanto, D. (2022). *Keamanan Data dalam Era Digitalisasi Perbankan***.** Yogyakarta: Gadjah Mada University Press.

Syekh Abdur, Pengadilan Agama, and Pangkalan Balai. "Nonmuslim Di Aceh Enforcement of Jinayat Law for Non-Muslims in Aceh." *Penegakan Hukum Jinayat Bagi Nonmuslim Di Aceh* 11 (2022): 21–42.

Wahyudi, T., & Nugroho, A. (2022). "Transformasi Digital di Sektor Perbankan: Peluang dan Tantangan." *Jurnal Transformasi Digital*, 8(1), 45–60.

Wijaya, B., & Hardianto, F. (2023). "Digital Banking Education: Bridging Financial Literacy and Inclusion." *International Journal of Financial Studies*, 11(1), 75–90.

Yustitiana, Rhesita. "Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian Dari Upaya Penegakan Hukum Di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum." *Jurnal Hukum Visio Justisia* 1, no. 1 (2021): 98–126.