JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 3 No: 2, April - Mei 2026
E-ISSN : 3046-4560

Tanggung Jawab Bank Atas Kerugian Nasabah Akibat Kejahatan Siber

The Bank's Liability For Customer Losses Resulting From Cybercrime

Cantika Reika Viana[1], Friska Adyla Naura[2*], Anna Yuliana[3], Salsa Nabilani[4], Muhammad Arya Yalhan[5], Baidhowi[6]
Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Negeri Semarang
Email : cantikareika90@students.unnes.ac.id[1], friskaadylanaura@students.unnes.ac.id[2], annayuliana1107@students.unnes.ac.id[3], salsanabilani@students.unnes.ac.id[4], aryayalhan@students.unnes.ac.id[5], baidhowi@mail.unnes.ac.id[6]

Article Info

Article history:
Received : 04-05-2026
Revised : 06-05-2026
Accepted : 08-05-2026
Pulished : 10-05-2026

Abstract

The development of digital banking services has increased the risk of cybercrime, which can result in losses for customers. This study aims to analyse the legal framework and legal protection against customer losses resulting from cybercrime in digital banking services. The method used is normative legal research employing a legislative and conceptual approach. The results of the study indicate that legal protection for customers is regulated through preventive and repressive mechanisms. Liability for losses is determined based on the source of the loss, which may be attributed to the banking service provider if caused by system weaknesses, or on a proportional basis if there is contributory negligence on the part of the customer. Although the regulations are adequate in theory, their implementation is still not optimal in providing effective protection for customers.

Keywords* : *Cybercrime, Digital banking, Customer protection

Abstrak

Perkembangan layanan perbankan digital meningkatkan risiko kejahatan siber yang dapat menimbulkan kerugian bagi nasabah. Penelitian ini bertujuan untuk menganalisis pengaturan hukum serta perlindungan hukum terhadap kerugian nasabah akibat kejahatan siber dalam layanan perbankan digital. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa perlindungan hukum bagi nasabah telah diatur melalui mekanisme preventif dan represif. Pembebanan tanggung jawab atas kerugian ditentukan berdasarkan sumber terjadinya kerugian, yang dapat dibebankan kepada pihak penyelenggara layanan perbankan apabila disebabkan oleh kelemahan sistem, atau secara proporsional apabila terdapat kontribusi kelalaian nasabah. Meskipun secara normatif regulasi telah memadai, implementasinya masih belum optimal dalam memberikan perlindungan yang efektif bagi nasabah.

Kata Kunci : Kejahatan siber, Perbankan digital, Perlindungan nasabah

PENDAHULUAN

Transformasi digital telah membawa perubahan fundamental dalam industri perbankan, khususnya melalui pengembangan layanan perbankan digital seperti internet banking, mobile banking, dan sistem pembayaran elektronik. Digitalisasi ini tidak hanya meningkatkan efisiensi dan kemudahan akses layanan keuangan bagi masyarakat, tetapi juga memperluas inklusi keuangan secara signifikan. Namun demikian, di balik kemajuan tersebut, muncul risiko baru yang semakin kompleks, terutama dalam bentuk kejahatan siber (*cybercrime)* yang menyasar sistem dan pengguna layanan perbankan digital.

Kejahatan siber dalam sektor perbankan berkembang dalam berbagai bentuk, seperti *phishing, skimming, malware, sniffing, hingga social engineering.* Modus-modus tersebut umumnya bertujuan untuk memperoleh data pribadi nasabah secara ilegal yang kemudian digunakan untuk melakukan transaksi tanpa izin dan menimbulkan kerugian finansial. Fenomena ini menunjukkan bahwa perkembangan teknologi digital tidak selalu diikuti dengan peningkatan keamanan yang memadai, sehingga membuka celah bagi pelaku kejahatan untuk mengeksploitasi kelemahan sistem maupun kelalaian pengguna (Hasanudin, dkk., 2024).

Dalam praktiknya, meningkatnya kasus kejahatan siber di sektor perbankan menimbulkan persoalan hukum yang krusial, yaitu mengenai tanggung jawab bank terhadap kerugian yang dialami nasabah. Hal ini menjadi kompleks karena dalam beberapa kasus, kerugian tidak hanya disebabkan oleh kelemahan sistem bank, tetapi juga oleh faktor kelalaian nasabah, seperti memberikan data pribadi kepada pihak yang tidak bertanggung jawab. Di sisi lain, bank sebagai penyelenggara layanan keuangan memiliki kewajiban untuk menjamin keamanan sistem serta melindungi data dan dana nasabah sebagai bentuk tanggung jawab profesional dan hukum.

Secara normatif, tanggung jawab bank dalam layanan digital di Indonesia telah diatur dalam berbagai regulasi, antara lain Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta peraturan dari Otoritas Jasa Keuangan (OJK). Dalam perkembangan terbaru, regulasi OJK menegaskan bahwa tanggung jawab bank bersifat langsung (*direct liability*) atas risiko yang timbul dari penggunaan layanan digital, termasuk akibat gangguan sistem dan serangan siber (Pesak, Verenly Yeremia, 2025). Hal ini menunjukkan bahwa secara prinsip, bank tidak dapat sepenuhnya melepaskan tanggung jawabnya kepada pihak lain, termasuk pihak ketiga penyedia teknologi.

Namun demikian, implementasi tanggung jawab tersebut dalam praktik masih menimbulkan berbagai perdebatan, terutama terkait batasan antara tanggung jawab bank dan tanggung jawab nasabah. Dalam kasus-kasus seperti phishing dan pembobolan mobile banking, seringkali terjadi perbedaan interpretasi mengenai pihak yang harus menanggung kerugian. Beberapa penelitian menunjukkan bahwa perlindungan hukum terhadap nasabah belum sepenuhnya optimal, baik dari aspek regulasi maupun penegakan hukum, sehingga menimbulkan ketidakpastian hukum bagi korban kejahatan siber (Widjana, dkk., 2025).

Berdasarkan latar belakang tersebut, penting untuk dilakukan kajian mendalam mengenai bagaimana konsep tanggung jawab bank dalam hukum perbankan digital, khususnya dalam konteks kerugian nasabah akibat kejahatan siber. Kajian ini diharapkan dapat memberikan pemahaman yang komprehensif mengenai konstruksi hukum yang berlaku, sekaligus memberikan kontribusi dalam penguatan perlindungan hukum bagi nasabah di era digital.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif yang menitikberatkan pada kajian terhadap norma hukum yang mengatur perlindungan konsumen dalam layanan perbankan digital, khususnya mengenai tanggung jawab bank atas kerugian nasabah akibat kejahatan siber. Penelitian hukum normatif dilakukan dengan menelaah peraturan perundang-undangan, doktrin, dan literatur hukum yang relevan. Menurut Soerjono Soekanto dan Sri Mamudji, penelitian hukum

normatif merupakan penelitian yang menggunakan data sekunder sebagai sumber utama dengan cara mengkaji bahan pustaka yang berkaitan dengan isu hukum yang diteliti.

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang berkaitan dengan perlindungan konsumen dan layanan perbankan digital, antara lain Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain itu, penelitian ini juga mengkaji kebijakan dan regulasi sektor jasa keuangan yang diterbitkan oleh Otoritas Jasa Keuangan dan Bank Indonesia terkait penyelenggaraan layanan perbankan digital dan perlindungan konsumen jasa keuangan.

Sumber hukum yang digunakan terdiri atas :

1. Sumber hukum primer berupa peraturan perundang-undangan,
2. Sumber hukum sekunder berupa buku, artikel jurnal, serta pendapat para ahli di bidang hukum siber dan perlindungan konsumen, serta
3. Sumber hukum tersier berupa kamus hukum dan ensiklopedia hukum.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan, sedangkan analisis bahan hukum menggunakan analisis kualitatif dengan pendekatan deskriptif-analitis, yaitu dengan mengkaji dan menafsirkan norma hukum yang berlaku untuk menjelaskan bentuk perlindungan hukum bagi nasabah serta konstruksi tanggung jawab bank dalam kasus kerugian nasabah akibat kejahatan siber dalam layanan perbankan digital.

Kerangka Teori Tanggung Jawab Hukum

Dalam menganalisis tanggung jawab bank atas kerugian nasabah akibat kejahatan siber, penelitian ini menggunakan tiga teori tanggung jawab hukum yang relevan.

a. Teori Tanggung Jawab Berdasarkan Kesalahan (*Fault-Based Liability* / *Liability Based on Fault*)

Teori ini berakar dari Pasal 1365 KUHPerdata yang menyatakan bahwa setiap perbuatan melawan hukum yang menimbulkan kerugian kepada orang lain mewajibkan pelakunya untuk mengganti kerugian tersebut. Menurut Ridwan H.R., tanggung jawab berdasarkan kesalahan mensyaratkan adanya empat unsur: perbuatan melawan hukum, kesalahan, kerugian, dan hubungan kausal antara kesalahan dan kerugian. Dalam konteks perbankan digital, teori ini diterapkan ketika bank terbukti lalai dalam menjaga keamanan sistem, misalnya tidak menerapkan autentikasi berlapis atau gagal mendeteksi transaksi mencurigakan (Ridwan H.R., 2011).

b. Teori Tanggung Jawab Langsung (*Direct Liability*)

Teori ini menegaskan bahwa bank sebagai penyelenggara layanan digital bertanggung jawab secara langsung atas segala risiko yang timbul dari penggunaan sistem yang mereka sediakan, tanpa dapat mengalihkan tanggung jawab tersebut kepada pihak ketiga seperti penyedia teknologi. Pesak (2025) menegaskan bahwa regulasi OJK telah mengadopsi prinsip *direct*

liability ini, sehingga bank tidak dapat melepaskan diri dari tanggung jawab hanya dengan alasan bahwa kelemahan berasal dari sistem pihak ketiga (Pesak, Verenly Yeremia, 2025).

c. Teori Tanggung Jawab Proporsional (*Proportional Liability*)

Dalam kasus-kasus di mana kerugian timbul akibat kombinasi antara kelemahan sistem bank dan kelalaian nasabah seperti dalam kasus *social engineering* tanggung jawab tidak dapat dibebankan sepenuhnya kepada satu pihak. Teori tanggung jawab proporsional mengatur bahwa pembebanan ganti rugi dilakukan secara berimbang sesuai dengan kadar kontribusi kesalahan masing-masing pihak. Teori ini relevan diterapkan dalam kasus phishing dan penipuan berbasis manipulasi psikologis, di mana nasabah turut berkontribusi dengan menyerahkan data rahasianya secara sukarela meskipun dalam keadaan tertipu (Fuady, Munir, 2013).

HASIL DAN PEMBAHASAN

1. Bentuk Perlindungan Hukum bagi Nasabah dalam Penggunaan Layanan Perbankan Digital

Sebagai pijakan utama, perlindungan hukum nasabah bank digital dibangun atas kerangka hukum nasional, yakni konstitusi dan serangkaian undang-undang serta peraturan pelaksana yang relevan. UUD 1945 (Pasal 28G) menjamin hak atas keamanan dan perlindungan diri, yang dilanjutkan dengan UU No. 8/1999 tentang Perlindungan Konsumen (UUPK) yang menegaskan kewajiban pelaku usaha (termasuk bank) memberikan kepastian perlindungan kepada konsumen. Pasal 7 huruf f UUPK khususnya mewajibkan pelaku usaha memberi kompensasi atau ganti rugi atas kerugian konsumen akibat penggunaan barang/jasa. Selain itu, UU Perbankan (sebelum UU No. 4/2023) di Pasal 29 ayat (4) menuntut setiap bank menyediakan informasi mengenai potensi risiko kerugian transaksi nasabah (D. Sinta, S. Zakia, & U. Safitri, 2020). Dalam konteks digital, UU No. 11/2008 tentang Informasi dan Transaksi Elektronik (ITE) juga memuat ketentuan pelindungan data pribadi, yang selanjutnya diperkuat oleh UU No. 27/2022 tentang Perlindungan Data Pribadi (PDPL). Dengan demikian, kerangka perundang-undangan memastikan bahwa nasabah memiliki hak atas keamanan dana dan data pribadi, serta hak memperoleh informasi yang transparan dan penyelesaian sengketa ketika dirugikan.

Selain undang-undang umum tersebut, Otoritas Jasa Keuangan (OJK) telah merumuskan aturan khusus tentang perbankan digital. POJK No.12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital menekankan prinsip kehati-hatian dan manajemen risiko, serta mewajibkan bank memenuhi prasyarat infrastruktur TI yang memadai guna keamanan transaksi (D. A. Astrini, 2015). Pasal 21 POJK ini secara eksplisit mengatur perlindungan konsumen pada layanan digital. Pasal 21 ayat (1) menegaskan setiap bank digital wajib menjalankan prinsip-prinsip perlindungan konsumen sesuai ketentuan di sektor jasa keuangan. Di ayat (2) ditegaskan bahwa bank harus memiliki sistem responsif dan mekanisme penanganan keluhan nasabah 24 jam sehari. Ayat (3) menyatakan tata cara perlindungan konsumen digital mengikuti pedoman perlindungan konsumen sektor jasa keuangan umum. Aturan turunan POJK ini (misalnya SEOJK No.17/2018) menguraikan agar bank menyediakan saluran pengaduan seperti telepon, email, atau surat, yang siap diakses nasabah setiap waktu. Dengan demikian, nasabah di perbankan digital mendapatkan perlindungan preventif dan represif yang komprehensif:

perlindungan preventif berupa penjelasan risiko dan jaminan kerahasiaan data, dan perlindungan represif berupa mekanisme ganti rugi serta penyelesaian sengketa atas kerugian layanan digital.

Untuk memperjelas konstruksi peristiwa hukum, kejahatan siber terhadap nasabah perbankan digital pada umumnya terjadi melalui tahapan berikut:

Tabel 1. Tahapan Kejahatan Siber

Tahap	Peristiwa	Pelaku	Peran/Perbuatan
1	Pengumpulan Data	Pelaku Kejahatan	Mencari target (nasabah) melalui media sosial, database bocor, dll
2	Pendekatan (social engineering/phishing)	Pelaku Kejahatan	Menghubungi korban (telepon, SMS, link palsu) untuk memperoleh data
3	Penyerahan Data	Nasabah	Memberikan OTP, PIN, password (sadar/tidak sadar)
4	Akses Sistem	Pelaku Kejahatan	Login ke akun mobile banking/internet banking
5	Eksekusi Transaksi	Pelaku Kejahatan	Transfer dana ke rekening tertentu
6	Kerugian Terjadi	Nasabah	Dana berkurang/menghilang
7	Respon Sistem	Bank	Mendeteksi/ gagal mendeteksi transaksi mencurigakan

Dari tabel ini terlihat bahwa kejahatan siber dalam perbankan tidak selalu murni kesalahan sistem, tetapi sering merupakan kombinasi antara:

a. Eksploitasi kelemahan sistem, dan/atau
b. Manipulasi psikologis terhadap nasabah (human error)

Prinsip-prinsip perlindungan konsumen yang harus dipenuhi oleh bank digital dirumuskan secara eksplisit dalam regulasi dan doktrin. Misalnya, OJK menyebut prinsip tersebut mencakup transparansi informasi layanan, perlakuan adil, keandalan layanan, serta kerahasiaan dan keamanan data konsumen. Artinya, bank wajib menyampaikan informasi produk, biaya, dan risiko secara terbuka; melayani nasabah secara tidak diskriminatif; serta menjaga keamanan dan kerahasiaan data pribadi dan finansial nasabah. Pasal 29 UU Perbankan (sebelum UU No.4/2023) sudah mengamanatkan kewajiban informasi mengenai risiko transaksi nasabah. Hal ini sangat penting karena layanan digital memunculkan ancaman siber baru; oleh karena itu, bank dituntut tidak hanya membangun sistem keamanan terkini tetapi juga membangun kepercayaan melalui transparansi dan perlindungan hukum yang kuat (A. Tasman & U. Ulfanora, 2023).

Di sisi lain, sebagai pelaku usaha jasa keuangan, bank juga tunduk pada norma UUPK yang melarang tindakan menyesatkan konsumen dan mewajibkan penerapan asas kehati-hatian nasabah (misalnya menjaga kerahasiaan kata sandi/OTP). Kajian normatif menegaskan bahwa selain perlindungan hukum eksplisit dalam UU 8/1999, prinsip kehati-hatian ('prudential') juga berfungsi sebagai bentuk perlindungan tidak langsung bagi nasabah.

Secara konkret, bentuk perlindungan preventif mencakup kewajiban bank memberikan edukasi dan informasi risiko transaksi digital. Bank diharuskan menerapkan otentikasi berlapis (two-factor authentication), enkripsi data, dan verifikasi kuat saat membuka akun nasabah. Misalnya, POJK 12/2018 menuntut penerapan faktor keamanan seperti biometrik atau token sebagai bagian dari verifikasi pelanggan (two-factor authentication). Bank juga wajib menyelenggarakan audit dan pengawasan internal untuk memitigasi potensi fraud (phishing, malware, skimming) serta menyaring pihak ketiga mitra mereka secara transparan. Dengan demikian, nasabah mendapatkan perlindungan preventif melalui peningkatan keamanan sistem bank dan informasi mengenai langkah-langkah keamanan yang harus mereka terapkan. Para peneliti menekankan bank perlu lebih aktif mengedukasi nasabah mengenai potensi kejahatan siber dan langkah antisipasi agar pengguna jasa digital lebih waspada.

Setelah terjadi kerugian akibat layanan perbankan digital, perlindungan hukum represif bagi nasabah diwujudkan melalui mekanisme klaim dan kompensasi. Secara normatif, Undang-Undang No. 8/1999 (UUPK) Pasal 7 huruf f mengamanatkan bahwa *"pelaku usaha wajib memberi kompensasi, ganti rugi, dan/atau penggantian atas kerugian akibat pemakaian barang dan/atau jasa"*. Artinya, jika nasabah dirugikan karena kelalaian sistem atau keamanan bank (misalnya bank gagal menjaga data nasabah), bank berkewajiban memulihkan kerugian tersebut dengan mengembalikan dana atau memberikan ganti rugi sesuai ketentuan hukum. Hak pemulihan ini berlaku sama bagi nasabah perbankan digital maupun konvensional, karena keduanya berada di bawah payung perlindungan konsumen yang sama (Tasman & Ulfanora, 2023). Dalam praktiknya, kelalaian bank dapat dipandang sebagai *wanprestasi* atau perbuatan melawan hukum (onrechtmatige daad). Misalnya, Pasal 1365 KUHPerdata menyebutkan bahwa *"setiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain menimbulkan kewajiban ganti rugi"*

Penelitian Larasati dan Cahyaningsih (2026) menegaskan bahwa kegagalan penerapan prinsip kehati-hatian (misalnya pengamanan sistem elektronik) memenuhi unsur perbuatan melawan hukum pasal 1365, sehingga bank diwajibkan membayar ganti rugi atas kerugian materiil nasabah (Larasati & Cahyaningsih, 2026). Dengan kata lain, jika nasabah membuktikan bahwa bank lalai dalam operasional atau pengamanan sistemnya, maka bank dapat digugat secara perdata untuk mengganti kerugian tersebut.

Secara praktis, nasabah dapat mengajukan klaim ganti rugi melalui jalur perdata (pengadilan) ataupun mekanisme alternatif. Dalam gugatan perdata wanprestasi, nasabah harus membuktikan empat unsur: adanya perjanjian atau kewajiban bank, kelalaian/wanprestasi bank, kerugian nasabah, dan hubungan sebab-akibat antara keduanya. Jika unsur-unsur ini terpenuhi, hakim dapat memerintahkan bank membayar ganti rugi (misalnya damnum emergens atau lucrum cessans) sesuai Pasal 1246-1247 KUHPerdata. Selain litigasi, penyelesaian sengketa konsumen keuangan juga dapat melalui Lembaga Alternatif Penyelesaian Sengketa (LAPS) OJK

atau mediasi. Peraturan OJK (misalnya Pasal 21 POJK 12/2018 dan Surat Edaran SEOJK 17/2018) mengatur kewajiban bank menyediakan mekanisme pengaduan dan menyelesaikan sengketa nasabah secara cepat, sederhana, dan gratis. Pendekatan ini menegaskan bahwa penyelesaian klaim nasabah digital mengikuti prosedur perlindungan konsumen standar.

Berdasarkan uraian di atas, perlindungan represif bagi nasabah bank digital mencakup:

a. Kompensasi/Klaim Ganti Rugi: Bank wajib mengganti kerugian nasabah berdasarkan UU Perlindungan Konsumen Pasal 7f atau KUHPerdata (Pasal 1365 dst.) jika lalai.
b. Gugatan Wanprestasi/PMH: Kelalaian bank di ranah perbankan dianggap perbuatan melawan hukum (Pasal 1365 KUHPerdata), menimbulkan kewajiban membayar ganti rugi.
c. Mekanisme Pengaduan: Nasabah dapat mengajukan klaim melalui jalur internal bank, LAPS OJK, atau pengadilan. Keberhasilan klaim tergantung pembuktian kelalaian bank dan kerugian yang dialami.

Sebagai ilustrasi, Tasman & Ulfanora (2023) menyimpulkan bahwa skema ganti rugi nasabah perbankan digital sepenuhnya merujuk pada aturan perlindungan konsumen yang berlaku. Artinya, tidak ada perbedaan hak bagi nasabah digital; selama ada kelalaian bank, nasabah memiliki hak hukum untuk mendapatkan kembali dananya. Dengan demikian, bentuk perlindungan hukum represif ini menekankan pemberian kompensasi kepada nasabah pasca-insiden melalui jalur hukum perdata dan mekanisme pengaduan konsumen yang baku.

Dalam praktik, OJK mensyaratkan bank mempunyai saluran pengaduan yang direspon cepat dan profesional. Setiap keluhan nasabah atas transaksi yang dipertanyakan harus ditangani sesuai pedoman OJK/BI. Jika penyelesaian internal tidak memuaskan, nasabah dapat mengakses Lembaga Alternatif Penyelesaian Sengketa (SJK) sektor jasa keuangan (misalnya OJK, Asosiasi, atau lembaga mediasi) sesuai POJK 61/2020. Dengan mekanisme ini, nasabah memiliki jalur administratif sebelum mengajukan gugatan perdata. Dalam proses hukum, pengadilan perdata juga berperan menegakkan hak nasabah berdasarkan UU Perbankan, UU Perlindungan Konsumen, dan UU PDP, terutama dalam perkara kelalaian bank. Meskipun demikian, batas tanggung jawab bank tidak mutlak: bank hanya bertanggung jawab sepanjang kerugian nasabah akibat kesalahan bank. Jika kerugian muncul karena kelalaian nasabah sendiri (misalnya memberi akses PIN/OTP ke pihak lain), bank dapat melepaskan diri dari kewajiban ganti rugi. Dengan kata lain, perlindungan hukum ini bersifat kasuistis dibuktikan berdasarkan situasi masing-masing kasus.

Intinya, perlindungan hukum bagi nasabah perbankan digital diwujudkan lewat gabungan aturan preventif dan represif. Secara preventif, regulasi mengharuskan bank menjamin keamanan sistem, transparansi, dan edukasi risiko kepada nasabah. Secara represif, nasabah dijamin hak mendapat kompensasi atas kerugian yang disebabkan oleh kegagalan bank, serta akses ke mekanisme pengaduan dan sengketa yang diatur OJK. Kerangka perlindungan ini mencerminkan upaya negara untuk menyeimbangkan hubungan yang timpang antara bank (lembaga kuat) dan nasabah (pihak rentan), sekaligus mengadaptasi hukum konsumen tradisional ke ranah digital. Semua instrumen hukum tersebut bertujuan meningkatkan kepercayaan publik pada layanan perbankan digital dan mengurangi potensi kerugian nasabah di era siber.

Untuk memperkuat analisis mengenai perlindungan hukum bagi nasabah dalam layanan perbankan digital, penting untuk terlebih dahulu memahami konstruksi faktual mengenai bagaimana kejahatan siber tersebut terjadi dalam praktik. Kejahatan siber dalam sektor perbankan digital pada umumnya tidak terjadi secara sederhana, melainkan melalui suatu rangkaian peristiwa yang melibatkan interaksi antara pelaku kejahatan, nasabah, dan sistem perbankan itu sendiri. Proses tersebut biasanya diawali dengan tahap pengumpulan informasi oleh pelaku kejahatan, baik melalui media sosial, kebocoran data, maupun metode lainnya. Setelah itu, pelaku melakukan pendekatan kepada korban melalui teknik social engineering seperti phishing, dengan tujuan memperoleh data rahasia seperti PIN, password, atau kode OTP.

Dalam tahap selanjutnya, nasabah baik secara sadar maupun karena tertipu memberikan informasi tersebut kepada pelaku. Data yang diperoleh kemudian digunakan oleh pelaku untuk mengakses sistem perbankan digital secara tidak sah dan melakukan transaksi finansial yang merugikan nasabah. Pada titik inilah kerugian terjadi, sementara sistem bank dalam beberapa kasus gagal mendeteksi adanya aktivitas yang mencurigakan. Rangkaian peristiwa ini menunjukkan bahwa kejahatan siber dalam perbankan digital tidak selalu disebabkan oleh satu faktor tunggal, melainkan merupakan kombinasi antara kelemahan sistem keamanan dan faktor kelalaian pengguna.

Dalam konteks tersebut, perlu dilakukan pembedaan konseptual yang tegas antara penipuan (fraud) dan peretasan siber (hacking), karena keduanya memiliki implikasi hukum yang berbeda, khususnya dalam menentukan pihak yang bertanggung jawab atas kerugian nasabah. Penipuan dalam layanan perbankan digital umumnya terjadi melalui mekanisme manipulasi psikologis, di mana pelaku tidak secara langsung membobol sistem, melainkan mengelabui nasabah agar secara sukarela memberikan akses terhadap akun mereka. Dalam hal ini, akses terhadap sistem diperoleh melalui persetujuan semu yang lahir dari tipu muslihat, sehingga unsur utama terletak pada perbuatan penipuan sebagaimana diatur dalam hukum pidana.

Sebaliknya, peretasan siber merupakan tindakan akses ilegal terhadap sistem elektronik tanpa persetujuan pengguna. Dalam kasus ini, pelaku secara aktif mengeksploitasi celah keamanan sistem perbankan, misalnya melalui malware, eksploitasi jaringan, atau teknik teknis lainnya. Perbedaan mendasar antara kedua bentuk kejahatan ini terletak pada sumber akses terhadap sistem: dalam penipuan, akses berasal dari korban, sedangkan dalam peretasan, akses berasal dari kelemahan sistem. Distingsi ini menjadi sangat penting karena menentukan arah pertanggungjawaban hukum.

Apabila kerugian nasabah timbul akibat peretasan sistem, maka secara prinsipil bank harus bertanggung jawab penuh, mengingat bank memiliki kewajiban hukum untuk menjamin keamanan sistem dan melindungi data serta dana nasabah. Kegagalan dalam menjaga keamanan sistem dapat dikualifikasikan sebagai bentuk kelalaian yang memenuhi unsur perbuatan melawan hukum sebagaimana diatur dalam Pasal 1365 KUHPerdata. Dalam hal ini, tanggung jawab bank bersifat dominan karena risiko yang timbul merupakan bagian dari risiko operasional yang berada dalam kendali bank sebagai penyedia layanan.

Namun demikian, dalam kasus penipuan berbasis social engineering, di mana nasabah secara aktif memberikan data rahasia kepada pihak lain, konstruksi tanggung jawab menjadi

lebih kompleks. Meskipun terdapat unsur kelalaian dari pihak nasabah, bank tidak serta merta dapat melepaskan tanggung jawabnya sepenuhnya. Hal ini dikarenakan bank tetap memiliki kewajiban untuk menyediakan sistem keamanan yang memadai, termasuk mekanisme deteksi transaksi mencurigakan (fraud detection system), edukasi kepada nasabah, serta sistem notifikasi yang responsif. Oleh karena itu, dalam situasi tertentu, tanggung jawab dapat bersifat proporsional dengan mempertimbangkan kontribusi kesalahan dari masing-masing pihak.

Dengan demikian, dapat dipahami bahwa penentuan tanggung jawab dalam kasus kejahatan siber di sektor perbankan digital bersifat kasuistis dan bergantung pada analisis terhadap sumber terjadinya akses ilegal. Apabila akses terjadi akibat kegagalan sistem, maka tanggung jawab berada pada bank, sedangkan apabila akses terjadi akibat kelalaian nasabah, maka tanggung jawab dapat dibagi. Pendekatan ini menunjukkan bahwa perlindungan hukum bagi nasabah tidak hanya bergantung pada keberadaan norma hukum, tetapi juga pada kemampuan untuk mengidentifikasi secara tepat karakteristik peristiwa hukum yang terjadi. Oleh karena itu, kejelasan dalam membedakan antara penipuan dan peretasan menjadi kunci dalam menciptakan kepastian hukum serta keadilan bagi para pihak yang terlibat.

2. Apakah regulasi yang ada telah memadai dalam menjamin keamanan dan perlindungan data nasabah?

Regulasi yang ada saat ini secara normatif telah memberikan kerangka perlindungan yang cukup memadai bagi nasabah dalam layanan perbankan digital, namun demikian kerangka tersebut belum sepenuhnya mampu menjamin keamanan dan perlindungan data nasabah secara efektif dalam praktik. Hal ini disebabkan oleh masih terdapatnya berbagai kelemahan, baik dalam aspek implementasi, koordinasi antar regulasi, maupun kemampuan adaptasi terhadap perkembangan teknologi yang semakin pesat. Data nasabah dalam sistem perbankan merupakan informasi yang bersifat sangat sensitif, karena tidak hanya mencakup identitas pribadi, tetapi juga informasi finansial yang apabila disalahgunakan dapat menimbulkan kerugian yang besar. Oleh karena itu, keberadaan regulasi yang tidak hanya lengkap secara normatif tetapi juga kuat secara implementatif menjadi sangat penting sebagai bentuk jaminan hukum sekaligus upaya menjaga kepercayaan masyarakat terhadap sistem perbankan. Dalam konteks ini, negara telah menghadirkan berbagai instrumen hukum, seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta berbagai regulasi yang dikeluarkan oleh Otoritas Jasa Keuangan. Selain itu, dalam praktik perbankan juga dikenal prinsip kepercayaan (fiduciary principle) dan prinsip kerahasiaan (confidential principle) yang menegaskan kewajiban bank dalam menjaga keamanan informasi nasabah. Hal ini menunjukkan bahwa secara normatif, sistem hukum Indonesia telah memiliki kerangka perlindungan yang cukup komprehensif dalam menjamin keamanan dan perlindungan data nasabah, meskipun dalam praktiknya masih menghadapi berbagai tantangan implementasi (Maisah, 2022).

Namun demikian, apabila ditinjau lebih lanjut, keberadaan regulasi tersebut belum sepenuhnya mampu menjamin perlindungan data nasabah secara efektif dalam praktik. Hal ini tercermin dari masih terjadinya berbagai kasus kebocoran data dalam sektor perbankan yang menunjukkan adanya kesenjangan antara norma hukum yang tertulis dengan pelaksanaannya di lapangan (Aziz, dkk., 2023). Fenomena ini mengindikasikan bahwa keberadaan regulasi belum secara otomatis menjamin efektivitas perlindungan data, terutama apabila tidak didukung oleh

mekanisme pengawasan yang kuat serta tingkat kepatuhan yang tinggi dari lembaga perbankan. Dalam konteks ini, dapat dikatakan bahwa perlindungan hukum terhadap data nasabah masih menghadapi permasalahan dalam aspek implementasi, sehingga regulasi yang ada belum mampu berfungsi secara optimal sebagai instrumen perlindungan. Lebih lanjut, kelemahan dalam implementasi regulasi juga terlihat dari belum optimalnya sistem pengawasan serta rendahnya tingkat kepatuhan terhadap standar perlindungan data yang telah ditetapkan. Dalam praktiknya, tidak semua lembaga perbankan memiliki kesiapan yang sama dalam hal keamanan sistem digital, sehingga masih terdapat celah yang dapat dimanfaatkan oleh pelaku kejahatan siber. Selain itu, mekanisme perlindungan bagi nasabah yang mengalami kerugian akibat kebocoran data juga belum berjalan secara maksimal, baik dalam hal pemulihan kerugian maupun kepastian hukum (Ichsandi, 2023). Kondisi ini menunjukkan bahwa regulasi yang ada masih memiliki kelemahan dalam aspek implementatif, sehingga belum mampu memberikan perlindungan yang menyeluruh dan efektif bagi nasabah sebagai konsumen jasa keuangan.

Di sisi lain, perkembangan teknologi informasi yang sangat pesat juga menjadi tantangan tersendiri bagi efektivitas regulasi yang ada. Transformasi digital dalam sektor perbankan telah membuka peluang bagi berbagai bentuk kejahatan siber yang semakin kompleks dan sulit dikendalikan. Metode kejahatan seperti phishing, malware, dan social engineering terus berkembang dengan tingkat kecanggihan yang semakin tinggi, sementara regulasi yang ada cenderung bersifat reaktif dan belum mampu mengantisipasi perkembangan tersebut secara optimal (Ahmad Rizki, 2023). Hal ini menunjukkan bahwa regulasi yang ada belum sepenuhnya adaptif terhadap dinamika teknologi, sehingga perlindungan data nasabah masih berada dalam posisi yang tertinggal dibandingkan dengan perkembangan ancaman siber yang ada. Selain permasalahan tersebut, terdapat pula isu mengenai ketidakjelasan pembagian tanggung jawab antara pihak bank dan nasabah dalam kasus kebocoran data. Dalam praktiknya, seringkali terjadi perbedaan pandangan terkait pihak yang harus bertanggung jawab atas kerugian yang timbul. Pihak bank cenderung mengaitkan kebocoran data dengan kelalaian nasabah, misalnya dalam menjaga kerahasiaan informasi pribadi, sementara nasabah beranggapan bahwa kebocoran tersebut merupakan akibat dari lemahnya sistem keamanan yang disediakan oleh bank. Ketidakjelasan ini menunjukkan bahwa regulasi yang ada belum memberikan batasan yang tegas mengenai tanggung jawab masing-masing pihak, sehingga berpotensi menimbulkan ketidakpastian hukum dan melemahkan posisi nasabah dalam hubungan hukum dengan lembaga perbankan. Permasalahan lain yang turut mempengaruhi efektivitas perlindungan data nasabah adalah lemahnya penegakan hukum serta pemberian sanksi terhadap pelanggaran. Meskipun berbagai ketentuan telah mengatur kewajiban perlindungan data, namun dalam praktiknya sanksi yang diberikan belum sepenuhnya memberikan efek jera, sehingga pelanggaran masih terus terjadi. Kondisi ini menunjukkan bahwa keberadaan regulasi belum diiringi dengan penegakan hukum yang kuat, yang seharusnya menjadi faktor penting dalam memastikan kepatuhan lembaga perbankan terhadap ketentuan yang berlaku. Selain itu, lemahnya penegakan hukum juga dapat berdampak pada menurunnya kepercayaan masyarakat terhadap sistem perbankan, yang pada akhirnya dapat mengganggu stabilitas sektor keuangan secara keseluruhan.

Selain itu, fragmentasi regulasi yang mengatur perlindungan data juga menjadi kendala dalam menciptakan sistem perlindungan yang efektif. Pengaturan mengenai perlindungan data nasabah saat ini tersebar dalam berbagai peraturan perundang-undangan yang berbeda, sehingga

berpotensi menimbulkan tumpang tindih dan ketidaksinkronan dalam implementasinya. Kondisi ini menunjukkan perlunya harmonisasi regulasi agar tercipta sistem perlindungan data yang lebih terintegrasi dan mudah diterapkan. Dalam konteks global, harmonisasi ini juga penting agar regulasi nasional dapat menyesuaikan diri dengan standar internasional dalam perlindungan data pribadi. Berdasarkan uraian tersebut, dapat disimpulkan bahwa regulasi yang ada saat ini belum sepenuhnya memadai dalam menjamin keamanan dan perlindungan data nasabah di sektor perbankan. Meskipun secara normatif telah tersedia berbagai ketentuan yang mengatur perlindungan data, namun secara implementatif masih terdapat berbagai kelemahan, baik dalam aspek pengawasan, kepatuhan, adaptasi terhadap perkembangan teknologi, maupun penegakan hukum. Oleh karena itu, diperlukan adanya pembaharuan hukum yang tidak hanya berfokus pada penyempurnaan norma, tetapi juga pada penguatan implementasi, peningkatan kualitas pengawasan, penegasan tanggung jawab hukum, serta peningkatan standar keamanan teknologi. Dengan demikian, perlindungan data nasabah dapat berjalan secara lebih efektif dan mampu memberikan jaminan kepastian hukum serta rasa aman bagi masyarakat dalam menggunakan layanan perbankan digital.

Selain permasalahan yang telah diuraikan sebelumnya, kompleksitas perlindungan data nasabah juga semakin meningkat seiring dengan berkembangnya ekosistem perbankan digital yang melibatkan berbagai pihak di luar institusi perbankan itu sendiri. Dalam praktiknya, pengelolaan data tidak hanya dilakukan oleh bank, tetapi juga melibatkan pihak ketiga seperti perusahaan fintech, penyedia layanan teknologi, hingga mitra kerja sama seperti asuransi. Keterlibatan banyak pihak ini secara langsung memperluas titik kerentanan terhadap kebocoran data, karena semakin banyak entitas yang memiliki akses terhadap informasi nasabah. Dalam kajian terkait kerjasama bancassurance, ditemukan bahwa belum adanya kejelasan pengaturan mengenai tanggung jawab antar pihak menyebabkan perlindungan data menjadi tidak optimal ketika terjadi pelanggaran (R. Putra dan A. Wijaya, 2023). Kondisi ini menunjukkan bahwa regulasi yang ada belum sepenuhnya mampu mengakomodasi kompleksitas hubungan hukum dalam ekosistem digital perbankan. Lebih lanjut, dalam perspektif perlindungan konsumen, posisi nasabah sebagai pengguna layanan perbankan masih berada pada kondisi yang lemah, terutama dalam menghadapi dominasi institusi keuangan yang memiliki kontrol penuh terhadap sistem dan informasi. Ketimpangan ini diperparah oleh rendahnya literasi digital masyarakat terkait keamanan data pribadi, sehingga nasabah seringkali tidak menyadari risiko yang dihadapi dalam penggunaan layanan perbankan digital, termasuk ancaman seperti phishing dan social engineering yang memanfaatkan kelengahan pengguna (Ichsandi, 2023). Dalam sebuah penelitian di bidang hukum ekonomi syariah, disebutkan bahwa perlindungan terhadap nasabah masih belum optimal karena belum adanya keseimbangan posisi antara pelaku usaha dan konsumen (S. Rahmawati, 2022). Hal ini menegaskan bahwa perlindungan data nasabah tidak hanya bergantung pada regulasi teknis, tetapi juga memerlukan pendekatan perlindungan konsumen yang lebih kuat.

Secara normatif, Indonesia telah memiliki instrumen hukum yang cukup komprehensif seperti UU PDP, UU ITE, hingga POJK No. 11/POJK.03/2022. Namun, jika dibedah menggunakan Teori Tanggung Jawab Mutlak (*Strict Liability*), masih terdapat celah hukum (*legal gap*) yang signifikan. Dalam perspektif Teori Tanggung Jawab Mutlak, bank seharusnya memikul beban pembuktian dan tanggung jawab penuh atas kerugian yang timbul dari kegagalan

sistem keamanan siber tanpa harus membuktikan adanya unsur kesalahan manual (*fault*). Namun, regulasi saat ini, khususnya dalam implementasi Pasal 1365 KUHPerdata, masih sering kali memberatkan nasabah untuk membuktikan adanya kesalahan dari pihak bank. Hal ini sangat sulit dilakukan oleh nasabah awam karena adanya ketimpangan akses informasi teknis (*information asymmetry*) terhadap sistem perbankan (Sinta, A. S., 2023).

Lebih lanjut, jika ditinjau dari Teori Tanggung Jawab Proporsional, regulasi yang ada belum secara tegas mengatur batasan tanggung jawab dalam kasus *social engineering*. Berikut adalah tabel perbandingan untuk mempertajam batasan tanggung jawab hukum tersebut:

Tabel 2. Perbandingan Tanggung Jawab Berdasarkan Sumber Akses Kejahatan

No	Aspek Perbandingan	Ancaman Berbasis Teknologi (Hacking/Malware)	Ancaman Berbasis Manusia (Social Engineering)
1	**Titik Lemah**	Celah Keamanan Sistem Bank	Kelalaian/Manipulasi Psikologis Nasabah
2	**Basis Teori**	*Strict Liability* (Tanggung Jawab Mutlak)	*Proportional Liability* (Proporsional)
3	**Beban Tanggung Jawab**	Bank Sepenuhnya	Berbagi (Bank & Nasabah)
4	**Alasan Hukum**	Bank gagal menjamin keamanan sistem yang mereka operasikan.	Terdapat kontribusi kelalaian nasabah, namun bank bertanggung jawab atas mitigasi transaksi.

Kelemahan regulasi saat ini juga terlihat dari sifatnya yang cenderung reaktif. Munculnya jenis kejahatan siber baru seperti serangan berbasis AI atau *deepfake* belum terakomodasi secara spesifik dalam UU ITE maupun POJK. Hal ini menyebabkan ketidakpastian hukum dalam menentukan apakah sebuah peristiwa merupakan murni kelalaian nasabah atau kegagalan bank dalam menyediakan sistem deteksi dini (*Fraud Detection System*). Oleh karena itu, diperlukan transformasi regulasi yang tidak hanya berfokus pada standar teknis, tetapi juga mewajibkan adanya mekanisme kompensasi otomatis bagi nasabah dalam kasus-kasus yang secara jelas merupakan kegagalan sistem (*system failure*), sejalan dengan prinsip kepercayaan (*fiduciary principle*) dalam hukum perbankan (Fajar, M., & Achmad, Y., 2022).

Dalam perkembangannya, teknologi yang semakin berkembang pesat tentu seperti yang sudah dibahas, yaitu menimbulkan tantangan baru dalam perlindungan data, khususnya dengan adanya penggunaan kecerdasan buatan (artificial intelligence) dan sistem berbasis algoritma dalam layanan perbankan. Teknologi ini memungkinkan pengolahan data dalam skala besar secara cepat, namun juga meningkatkan risiko penyalahgunaan data apabila tidak diimbangi dengan sistem keamanan yang memadai. Dalam kajian hukum teknologi informasi, disebutkan bahwa penggunaan teknologi digital dalam sektor keuangan justru meningkatkan potensi pelanggaran data apabila tidak diikuti dengan regulasi yang adaptif dan sistem pengamanan yang kuat (I. K. Adnyana, 2023). Hal ini menunjukkan bahwa perkembangan teknologi tidak selalu sejalan dengan kesiapan regulasi dalam memberikan perlindungan. Selain itu, meningkatnya intensitas kejahatan siber juga menjadi indikator bahwa data nasabah telah menjadi target utama dalam berbagai bentuk kejahatan digital. Berbagai kasus menunjukkan bahwa serangan seperti

ransomware dan peretasan sistem perbankan dapat menyebabkan kebocoran data dalam skala besar, yang pada akhirnya merugikan nasabah. Dalam studi terkait serangan siber di sektor perbankan, ditemukan bahwa kelemahan sistem keamanan dan kurangnya kesiapan institusi menjadi faktor utama terjadinya insiden kebocoran data. Kondisi ini menegaskan bahwa perlindungan data tidak cukup hanya diatur secara normatif, tetapi juga harus didukung oleh kesiapan teknis dan kelembagaan yang memadai.

Selanjutnya, dalam konteks globalisasi, perlindungan data nasabah juga menghadapi tantangan berupa arus data lintas negara yang semakin sulit dikendalikan. Transaksi perbankan digital memungkinkan terjadinya transfer data ke luar yurisdiksi nasional, sehingga menimbulkan persoalan terkait dengan perlindungan hukum yang berlaku. Dalam kajian mengenai perbankan digital, disebutkan bahwa belum optimalnya harmonisasi antara regulasi nasional dengan standar internasional menjadi salah satu kendala dalam perlindungan data nasabah (D. Pratama, 2023). Oleh karena itu, diperlukan upaya untuk menyesuaikan regulasi nasional dengan prinsip-prinsip global agar perlindungan data dapat dilakukan secara lebih efektif. Dengan demikian, dapat dilihat bahwa permasalahan perlindungan data nasabah dalam sektor perbankan tidak hanya berkaitan dengan keberadaan regulasi, tetapi juga dipengaruhi oleh kompleksitas ekosistem digital, perkembangan teknologi, serta dinamika hubungan antara pelaku usaha dan konsumen. Hal ini menunjukkan bahwa pembaharuan regulasi harus dilakukan secara komprehensif dengan memperhatikan berbagai aspek tersebut, sehingga mampu memberikan perlindungan yang lebih efektif dan adaptif terhadap perkembangan zaman.

KESIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan bahwa perlindungan hukum bagi nasabah dalam layanan perbankan digital telah diatur melalui berbagai peraturan perundang-undangan yang mencakup aspek preventif dan represif. Perlindungan preventif diwujudkan melalui kewajiban penyedia layanan perbankan dalam menjaga keamanan sistem, transparansi informasi, serta edukasi kepada nasabah, sedangkan perlindungan represif diberikan melalui mekanisme pengaduan, penyelesaian sengketa, dan pemberian ganti rugi atas kerugian yang timbul. Pembebanan tanggung jawab atas kerugian nasabah akibat kejahatan siber tidak bersifat mutlak, melainkan ditentukan berdasarkan sumber terjadinya kerugian. Dalam hal kerugian disebabkan oleh kelemahan sistem atau kegagalan pengamanan, maka tanggung jawab dapat dibebankan kepada pihak penyelenggara layanan perbankan. Namun, apabila kerugian terjadi akibat kelalaian nasabah, maka pembebanan tanggung jawab dapat dilakukan secara proporsional dengan mempertimbangkan kontribusi masing-masing pihak. Meskipun secara normatif regulasi yang ada telah cukup memadai, dalam praktiknya masih terdapat berbagai kendala, seperti lemahnya implementasi, kurang optimalnya pengawasan, serta belum adanya kejelasan batas tanggung jawab dalam beberapa kasus kejahatan siber. Oleh karena itu, diperlukan penguatan dalam aspek implementasi regulasi, peningkatan sistem keamanan, serta kejelasan pengaturan mengenai pembagian tanggung jawab agar perlindungan hukum bagi nasabah dapat berjalan secara lebih efektif dan memberikan kepastian hukum.

DAFTAR PUSTAKA

Adnyana, I. K. (2022). Perlindungan Data Pribadi dalam Penggunaan Teknologi Artificial Intelligence di Sektor Keuangan. *Jurnal Komunikasi Hukum Universitas Pendidikan Ganesha*, 8(2).

Astrini, D. A. (2015). Perlindungan Hukum Nasabah Internet Banking. *Lex Privatum*.

Aziz, dkk. (2023). Analisis Perlindungan Data Nasabah dalam Sistem Perbankan di Indonesia. *Jurnal Ilmu Hukum*, 6(2).

Fajar, M., & Achmad, Y. (2022). *Dualisme Penelitian Hukum Normatif & Empiris*. Yogyakarta: Pustaka Pelajar.

Fuady, Munir. (2013). *Perbuatan Melawan Hukum: Pendekatan Kontemporer*. Bandung: Citra Aditya Bakti.

Hasanudin, T. A. (2024). Perlindungan Nasabah dan Tanggung Jawab Bank dalam Penanggulangan Kejahatan Digital Berbasis Social Engineering. *Indonesia Journal of Business Law*.

Hidayat, M. F. (2023). Analisis Serangan Siber dan Perlindungan Data Nasabah pada Sektor Perbankan Indonesia. *Jurnal Staatsrecht UIN Sunan Kalijaga*, 4(2).

Ichsandi. (2023). Tantangan Perlindungan Data Pribadi dalam Era Kejahatan Siber. *Jurnal Hukum Teknologi Informasi*, 5(1).

Larasati & Cahyaningsih. (2026). Perlindungan Hukum Nasabah atas Kelalaian Sistem Digital.

Maisah. (2022). Perlindungan Data Pribadi Nasabah dalam Layanan Perbankan Digital. *Jurnal Hukum dan Perbankan*, 4(1).

Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum.

Pesak, V. Y. (2025). Tanggung Jawab Hukum Bank Umum atas Risiko Layanan Digital Berdasarkan POJK. *Lex Crimen*.

Pratama, D. (2023). Tantangan Regulasi dan Keamanan Data pada Bank Digital di Indonesia. *Causa: Jurnal Hukum dan Keuangan*, 2(1).

Prihandana R., Hendroko R. & Nuramin M. (2006). *Menghasilkan Biodiesel Murah Mengatasi Polusi dan Kelangkaan BBM*. Jakarta: PT. Agromedia Pustaka.

Putra, R., & Wijaya, A. (2023). Tanggung Jawab Hukum dalam Perlindungan Data Nasabah pada Kerjasama Bancassurance. *Jurnal Media Akademik*, 5(2).

Rahmawati, S. (2022). Perlindungan Konsumen dalam Layanan Perbankan Digital Perspektif Hukum Ekonomi Syariah. *Jurnal Istiqomah*, 3(1).

Ridwan H.R. (2010). *Hukum Administrasi Negara*. Jakarta: Raja Grafindo Persada.

Rizki, A. (2023). Analisis Kebocoran Data Nasabah pada Kasus Bank Syariah Indonesia. *Jurnal Hukum dan Keuangan Syariah*, 3(2).

Sinta, A. S. (2023). *Efektivitas Perlindungan Data Pribadi Nasabah Perbankan dalam Era Cyber Crime*. Jakarta: Sinar Grafika.

Sinta, D., Zakia, S., & Safitri, U. (2020). Analisis Perlindungan Hukum Bagi Nasabah Digital. *Jurnal Ilmu Wawasan Publik (JIWP)*.

Tasman, A., & Ulfanora, U. (2023). Perlindungan Hukum Nasabah Bank Digital. *UNES Law Review*.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

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

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Widjana, N. P. J. M. P., dkk. (2025). Pertanggungjawaban Bank terhadap Kerugian Nasabah Akibat Phishing. *Jurnal Konsep Ilmu Hukum*.