

Perlindungan Hukum Nasabah Bank Terhadap Adanya Kebocoran Data Pribadi Dihubungkan Dengan Asas Kerahasiaan Bank (Studi Kasus Kebocoran Data Bank Syariah Indonesia Tahun 2023)

Arfan Hamdani¹, Agus Prihartono², Rani Sri Agustina³

Fakultas Hukum Universitas Sultan Ageng Tirtayasa

Korespondensi Email : arfanhamdani98@gmail.com

Abstract

The rapid development of digital technology within the banking sector has enhanced financial transactions. However, it triggers critical risks to the security of customers' personal data. The system disruptions and alleged data breaches experienced by Bank Syariah Indonesia in 2023 cause legal issues concerning personal data protection, corporate liability, and the enforcement of the principle of bank secrecy within the digital banking ecosystem. The purpose of this research is to analyze legal protection of customer's personal data breaches and legal responsibility of the bank using bank secrecy principle. This research utilizes normative legal research with a statutory approach, conceptual approach and case approach. Primary, secondary and tertiary sources are used as legal materials. The legal materials are analyzed qualitatively. The results show that although the legal protection of customers against personal data breaches has been regulated in the Personal Data Protection Law, the Banking Law, the Sharia Banking Law, and various regulations in the financial services sector, the protection is still not optimal. This is because of systemic failures in electronic system security regulations, obscure banking liability mechanisms and insufficient improvement for victims of data breaches. Moreover, the principle of bank secrecy needs to be reinvented in the digital age. The bank should not only serve as a safeguard for the customers' deposits but it must also fully incorporate the protection of customers' electronic personal data. This study concludes that banks, in their capacity as personal data controllers, have a strict legal responsibility to secure customer data and maintain electronic system integrity. Consequently, solid regulatory reinforcement, enhanced banking cybersecurity, and more effective control are imperative to guarantee genuine legal protection for customers within Indonesia's digital banking framework.

Keywords: Legal Protection, Personal Data, Customers, Bank Principle Secrecy, Digital Banking

Abstrak

Perkembangan teknologi digital dalam sektor perbankan memberikan kemudahan dalam pelayanan transaksi keuangan, namun juga menimbulkan risiko terhadap keamanan data pribadi nasabah. Kasus gangguan sistem dan dugaan kebocoran data yang dialami oleh Bank Syariah Indonesia Tahun 2023 menimbulkan persoalan hukum terkait perlindungan data pribadi, tanggung jawab dan pelaksanaan asas kerahasiaan

bank dalam sistem perbankan digital. Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap nasabah atas kebocoran data pribadi serta menganalisis tanggung jawab hukum bank dalam perspektif asas kerahasiaan bank. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Sumber bahan hukum terdiri atas bahan hukum primer, sekunder, dan tersier yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap nasabah atas kebocoran data pribadi telah diatur dalam Undang-Undang Perlindungan Data Pribadi, Undang-Undang Perbankan, Undang-Undang Perbankan Syariah, dan berbagai regulasi sektor jasa keuangan. Namun demikian, perlindungan tersebut masih belum optimal karena masih terdapat kelemahan dalam pengaturan keamanan sistem elektronik, mekanisme tanggung jawab bank, dan perlindungan terhadap korban kebocoran data pribadi. Selain itu, asas kerahasiaan bank dalam era digital tidak hanya mencakup kerahasiaan simpanan nasabah, tetapi juga mencakup perlindungan data pribadi elektronik nasabah. Penelitian ini menyimpulkan bahwa bank sebagai pengendali data pribadi memiliki tanggung jawab hukum terhadap perlindungan data nasabah dan keamanan sistem elektronik. Oleh karena itu, diperlukan penguatan regulasi, peningkatan keamanan siber perbankan, dan pengawasan yang lebih efektif untuk memberikan perlindungan hukum terhadap nasabah dalam sistem perbankan digital di Indonesia.

Kata Kunci: Perlindungan Hukum, Data Pribadi, Nasabah, Asas Kerahasiaan Bank, Perbankan Digital

Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan mendasar dalam berbagai sektor kehidupan termasuk dalam kegiatan ekonomi dan keuangan. Salah satu sektor yang mengalami transformasi paling cepat adalah perbankan. Layanan perbankan yang sebelumnya dilakukan secara tatap muka kemudian dalam perkembangannya bergeser ke kanal digital.

Hubungan hukum antara bank dan nasabah pada dasarnya dibangun atas dasar kepercayaan. Nasabah mempercayakan dana dan informasi pribadinya kepada bank untuk dikelola secara aman dan bertanggung jawab. Dalam dunia perbankan, kepercayaan masyarakat merupakan modal utama bagi keberlangsungan sistem keuangan. Tanpa adanya kepercayaan dari masyarakat, maka fungsi bank sebagai lembaga penghimpun dan penyalur dana tidak dapat berjalan secara optimal (Abd. Shomad dan Trisadini P. Usanti, 2016).

Prinsip kerahasiaan bank (*bank secrecy*) sejak lama diakui sebagai salah satu pilar utama kepercayaan publik terhadap lembaga perbankan. Kepercayaan tersebut menjadi modal sosial yang sangat penting karena tanpa kepercayaan sistem perbankan tidak dapat berfungsi secara optimal (Adrian Sutedi, 2022). Bank konvensional dan bank syariah memiliki persamaan terutama dalam sisi teknis penerimaan uang, mekanisme transfer, teknologi komputer yang digunakan, syarat-syarat umum untuk memperoleh pembiayaan seperti KTP, NPWP, proposal dan laporan keuangan. Akan tetapi, terdapat banyak perbedaan mendasar diantara keduanya. Perbedaan ini menyangkut aspek legal,

struktur organisasi, usaha yang dibiayai dan lingkungan kerja (Muhammad Syafii Antonio, 2019).

Asas kerahasiaan bank tidak lagi hanya berkaitan dengan larangan membuka informasi nasabah kepada pihak lain, tetapi juga mencakup kewajiban bank dalam menjaga keamanan sistem elektronik dari ancaman kebocoran data dan serangan siber. Hal ini menjadi semakin penting karena digitalisasi perbankan menyebabkan seluruh data nasabah tersimpan dan diproses melalui sistem elektronik yang rentan terhadap peretasan, malware, ransomware, maupun bentuk akses ilegal lainnya. Dengan demikian, perlindungan data pribadi nasabah tidak hanya menjadi persoalan teknis keamanan informasi, tetapi juga menjadi persoalan hukum yang berkaitan dengan tanggung jawab lembaga perbankan terhadap nasabah sebagai pemilik data pribadi (Budi Agus Riswandi, 2023)

Instrumen hukum yang mengatur mengenai perlindungan nasabah dan kewajiban bank dalam menjaga kerahasiaan data juga diatur dalam Undang-Undang Perbankan, Undang-Undang Perbankan Syariah dan Undang-Undang Pengembangan dan Penguatan Sektor Keuangan (P2SK). Ketentuan tersebut menunjukkan bahwa perlindungan terhadap data dan informasi nasabah merupakan kewajiban hukum yang harus dilaksanakan oleh bank. Tata kelola keamanan informasi pada penyelenggaraan jasa keuangan diatur dalam Pasal 1 angka 14 Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan yang menyebutkan *Pertama*, "Bank dan pihak terafiliasi wajib merahasiakan informasi mengenai nasabah penyimpan dan simpanannya." *Kedua*, dalam hal nasabah penyimpan sekaligus nasabah debitur, bank dan pihak terafiliasi wajib merahasiakan informasi mengenai nasabah dalam kedudukannya sebagai nasabah penyimpan." Serta Pasal 2 ayat (1) Peraturan Otoritas Jasa Keuangan Nomor 44 Tahun 2024 Tentang Rahasia Bank yang menyebutkan "Bank dan pihak terafiliasi wajib merahasiakan informasi mengenai nasabah penyimpan dan simpanannya dan/atau nasabah investor dan investasinya."

Permasalahan kebocoran data pribadi dalam sektor perbankan menjadi perhatian serius setelah terjadinya kasus kebocoran data dan gangguan sistem yang dialami oleh Bank Syariah Indonesia (BSI) pada tahun 2023. Gangguan layanan yang terjadi pada Bank Syariah Indonesia menyebabkan nasabah mengalami kesulitan dalam melakukan transaksi keuangan melalui berbagai layanan digital perbankan. Dalam perkembangannya, muncul dugaan bahwa gangguan tersebut disebabkan oleh serangan ransomware yang mengakibatkan kebocoran sejumlah data internal dan data nasabah Bank Syariah Indonesia.

Kasus tersebut menimbulkan kekhawatiran masyarakat mengenai keamanan data pribadi yang disimpan dalam sistem elektronik perbankan serta memunculkan pertanyaan mengenai bentuk perlindungan hukum dan tanggung jawab bank terhadap nasabah yang dirugikan akibat kebocoran data pribadi. Menurut Kamus Besar Bahasa Indonesia (KBBI), kebocoran berasal dari kata "bocor" yang berarti berlubang sehingga cairan, udara, atau isi keluar dari tempatnya. Dalam konteks informasi dan teknologi

digital, kebocoran data dapat diartikan sebagai keluarnya atau tersebarnya data dan informasi kepada pihak yang tidak berwenang (*Kamus Besar Bahasa Indonesia*, n.d.). Dengan demikian, kebocoran data pribadi dapat dipahami sebagai terbukanya atau tersebarnya data pribadi seseorang kepada pihak lain tanpa hak dan tanpa persetujuan dari pemilik data pribadi atau secara harfiah dipahami sebagai keadaan dimana sebuah rahasia tersiar atau terungkap ke publik.

Kasus gangguan sistem dan dugaan kebocoran data yang dialami oleh Bank Syariah Indonesia pada Tahun 2023 menjadi salah satu peristiwa penting dalam perkembangan sistem perbankan digital di Indonesia. Kasus tersebut memperoleh perhatian luas dari masyarakat karena menyebabkan terganggunya berbagai layanan perbankan digital dan menimbulkan kekhawatiran mengenai keamanan data pribadi nasabah dalam sistem elektronik perbankan.

Gangguan sistem pada Bank Syariah Indonesia mulai terjadi sekitar awal bulan Mei 2023. Pada saat itu, sejumlah nasabah mengeluhkan tidak dapat mengakses berbagai layanan perbankan seperti mobile banking, internet banking, ATM, maupun layanan transaksi elektronik lainnya.

Mengutip berita CNN Indonesia, gangguan tersebut menyebabkan nasabah mengalami kesulitan dalam melakukan transaksi keuangan, pengecekan saldo, transfer dana, serta berbagai aktivitas layanan perbankan digital lainnya. Berbagai keluhan nasabah mulai tersebar melalui media sosial dan pemberitaan media massa. Banyak nasabah menyampaikan bahwa layanan BSI Mobile mengalami error dan tidak dapat digunakan secara normal. Selain itu, beberapa mesin ATM juga mengalami gangguan sehingga menyebabkan terganggunya aktivitas transaksi masyarakat yang menggunakan layanan Bank Syariah Indonesia.

Berita ini juga dikutip oleh Tempo.com bahwa gangguan sistem yang terjadi secara luas dan berlangsung dalam beberapa hari menyebabkan munculnya kekhawatiran masyarakat mengenai keamanan sistem elektronik Bank Syariah Indonesia. Bank Syariah Indonesia merupakan salah satu bank syariah terbesar di Indonesia dengan jumlah nasabah yang besar dan layanan digital yang luas, gangguan sistem tersebut menimbulkan dampak yang cukup signifikan terhadap aktivitas transaksi masyarakat. Kasus Bank Syariah Indonesia Tahun 2023 juga menimbulkan dugaan terjadinya kebocoran data pribadi nasabah. Dugaan tersebut muncul setelah beredarnya informasi mengenai data internal dan data nasabah yang diduga berhasil diakses oleh pihak yang melakukan serangan siber terhadap sistem Bank Syariah Indonesia.

Informasi mengenai dugaan kebocoran data Bank Syariah Indonesia kemudian menyebar luas melalui berbagai media sosial, forum digital, dan pemberitaan media massa. Beberapa pihak menyebutkan bahwa data hasil dugaan serangan siber terhadap Bank Syariah Indonesia diperjualbelikan atau dipublikasikan melalui forum digital tertentu dan *dark web*.

Penyebaran informasi tersebut semakin meningkatkan kekhawatiran masyarakat mengenai keamanan data pribadi dalam layanan digital perbankan. Banyak nasabah mulai mempertanyakan sejauh mana perlindungan yang diberikan oleh bank terhadap data pribadi dan informasi keuangan nasabah dalam sistem elektronik. Dalam perkembangan kasus tersebut, berbagai pihak, termasuk pemerintah dan otoritas terkait, mulai melakukan koordinasi dan investigasi terhadap dugaan serangan siber dan kebocoran data yang dialami oleh Bank Syariah Indonesia. Kasus tersebut kemudian menjadi salah satu perhatian penting dalam pembahasan mengenai keamanan siber, perlindungan data pribadi, dan perlindungan konsumen sektor jasa keuangan di Indonesia. Kasus kebocoran data Bank Syariah Indonesia menunjukkan bahwa perkembangan teknologi digital di sektor perbankan belum sepenuhnya diimbangi dengan sistem perlindungan data dan keamanan siber yang memadai. Kebocoran data pribadi nasabah tidak hanya berdampak pada terganggunya operasional bank, tetapi juga dapat menurunkan tingkat kepercayaan masyarakat terhadap sistem perbankan nasional. Dalam konteks hukum, kebocoran data pribadi menimbulkan persoalan mengenai sejauh mana bank bertanggung jawab atas keamanan data nasabah yang berada dalam penguasaannya serta bagaimana bentuk perlindungan hukum yang dapat diberikan kepada nasabah sebagai korban kebocoran data pribadi (Sinta Dewi Rosadi, 2023)

Penelitian mengenai perlindungan data pribadi nasabah perbankan telah dilakukan oleh beberapa peneliti. Salah satunya ditulis oleh Muhammad Faisal Aziz dkk (2025) dengan judul *Perlindungan Hukum terhadap Nasabah atas Penyalahgunaan Data Pribadi oleh Pihak Bank di Era Digitalisasi Perbankan*. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap nasabah masih belum efektif, masih lemahnya pengawasan, kurangnya kepatuhan bank terhadap prinsip kehati-hatian, dan belum optimalnya mekanisme pemulihan hak nasabah (Muhammad Faisal Aziz dkk, 2025).

Penelitian sebelumnya mengenai perlindungan data pribadi nasabah perbankan masih berfokus pada aspek perlindungan data pribadi secara umum dan belum secara khusus mengkaji hubungan antara kebocoran data pribadi nasabah dengan asas kerahasiaan bank serta pertanggungjawaban hukum bank dalam perspektif *strict liability*. Oleh karena itu, penelitian ini memiliki kebaruan (*novelty*) dalam mengkaji perlindungan hukum terhadap nasabah atas kebocoran data pribadi dengan menempatkan asas kerahasiaan bank sebagai perspektif utama dalam menganalisis pertanggungjawaban hukum bank terhadap nasabah.

Metode

Penelitian ini menggunakan penelitian yuridis normatif atau penelitian hukum normatif dengan pendekatan Perundang-undangan (*Statute Approach*). Penelitian hukum normatif adalah proses penelitian untuk meneliti dan mengkaji tentang hukum sebagai norma, aturan, asas hukum, prinsip hukum, doktrin hukum, teori hukum dan kepustakaan lainnya untuk menjawab permasalahan hukum yang diteliti (Muhaimin,

2020). Metode yuridis normatif digunakan dalam penelitian ini karena permasalahan yang diteliti berkaitan dengan perlindungan hukum terhadap nasabah atas kebocoran data pribadi dalam sektor perbankan yang dianalisis berdasarkan ketentuan peraturan perundang-undangan, asas hukum, teori hukum, serta doktrin hukum yang berkaitan dengan perlindungan data pribadi dan asas kerahasiaan bank. Penelitian ini tidak menitikberatkan pada penelitian lapangan, melainkan lebih berfokus pada pengkajian norma hukum yang mengatur perlindungan data pribadi nasabah dan pertanggungjawaban bank terhadap kebocoran data pribadi.

Sumber data yang digunakan dalam penelitian ini adalah data sekunder dan data primer sebagai penunjang. Data sekunder yaitu data yang diperoleh dari studi kepustakaan antara lain mencakup dokumen-dokumen resmi, buku-buku, hasil-hasil penelitian berwujud laporan, buku harian dan seterusnya yang berkaitan dan relevan dengan objek penelitian (Iqbal Hasan, 2022).

Hasil dan Diskusi

Perlindungan Hukum Nasabah Terhadap Adanya Kebocoran Data Pribadi

Indonesia sebagai negara hukum memiliki kewajiban untuk memberikan perlindungan terhadap hak-hak masyarakat, termasuk perlindungan terhadap data pribadi sebagai bagian dari hak privasi warga negara. Perlindungan terhadap data pribadi pada dasarnya merupakan bagian dari perlindungan hak asasi manusia yang dijamin oleh konstitusi. Perkembangan teknologi informasi dan digitalisasi sektor perbankan menyebabkan data pribadi masyarakat tersimpan dan diproses melalui sistem elektronik yang rentan terhadap ancaman penyalahgunaan data maupun kebocoran data pribadi. Oleh karena itu, negara melalui perangkat hukum berkewajiban memberikan perlindungan hukum terhadap masyarakat atas segala bentuk pelanggaran terhadap data pribadi, khususnya dalam sektor jasa keuangan dan perbankan (Satjipto Rahardjo, 2009).

Konsep perlindungan hukum tidak dapat dipisahkan dari keberadaan hak asasi manusia. Perlindungan hukum hadir sebagai bentuk perlindungan negara terhadap hak-hak individu agar tidak terjadi tindakan sewenang-wenang yang dapat merugikan masyarakat. Dalam perkembangan hukum modern, perlindungan hukum menjadi instrumen penting dalam menjaga keseimbangan hubungan hukum antara individu dengan negara maupun antara individu dengan pihak lainnya, termasuk hubungan hukum dalam sektor jasa keuangan dan perbankan (CST Kansil, 2011).

Perlindungan hukum pada dasarnya memiliki tujuan untuk menciptakan keadilan, kepastian hukum, dan kemanfaatan hukum bagi masyarakat. Keadilan dimaksudkan agar setiap orang memperoleh perlakuan yang sama di hadapan hukum dan mendapatkan perlindungan atas hak-haknya. Kepastian hukum bertujuan memberikan jaminan terhadap keberlakuan hukum secara jelas dan konsisten sehingga masyarakat mengetahui hak dan kewajibannya. Sementara itu, kemanfaatan hukum

bertujuan agar hukum dapat memberikan manfaat nyata bagi kehidupan masyarakat (Sudikno Mertokusumo, 2010) .

Perkembangan digitalisasi perbankan telah membawa perubahan besar terhadap sistem pelayanan jasa keuangan di Indonesia. Layanan perbankan yang sebelumnya dilakukan secara konvensional kini berkembang menjadi layanan berbasis digital seperti mobile banking, internet banking, dan berbagai transaksi elektronik lainnya. Perubahan tersebut menyebabkan meningkatnya penggunaan dan pengelolaan data pribadi nasabah dalam sistem elektronik perbankan. Dalam praktiknya, data pribadi nasabah memiliki nilai yang sangat penting karena berkaitan dengan identitas, transaksi keuangan, dan keamanan finansial nasabah. Kondisi tersebut menjadikan data pribadi sebagai objek yang sangat rentan terhadap tindak kejahatan siber seperti peretasan, ransomware, pencurian data, maupun penyalahgunaan informasi pribadi oleh pihak yang tidak berwenang (Rika Ratna Sembiring, 2023).

Prinsip kerahasiaan mengartikan bahwa data pribadi seorang nasabah harus dijaga kerahasiaannya terutama di era perbankan digital sekarang ini. Berdasarkan Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum, pemanfaatan perkembangan teknologi informasi secara optimal merupakan persyaratan dalam mendukung inovasi layanan bank. Oleh karena itu layanan perbankan digital sekarang ini semakin banyak digunakan oleh bank.

Sebagai penyedia layanan perbankan digital tentunya sebuah bank harus memperhatikan syarat-syarat seperti yang diatur dalam Pasal 24 Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang Bank Umum, yaitu: memiliki model bisnis dengan penggunaan teknologi yang inovatif dan aman dalam melayani kebutuhan nasabah; memiliki kemampuan untuk mengelola model bisnis perbankan digital yang pruden dan berkesinambungan; memiliki manajemen risiko secara memadai; memenuhi aspek tata kelola termasuk pemenuhan Direksi yang mempunyai kompetensi di bidang teknologi informasi dan kompetensi lain sesuai dengan ketentuan OJK mengenai penilaian kemampuan dan kepatutan bagi pihak utama lembaga jasa keuangan; menjalankan perlindungan terhadap keamanan data nasabah; dan memberikan upaya yang kontributif terhadap perkembangan ekosistem keuangan digital dan/atau inklusi keuangan.

Berdasarkan syarat tersebut, dapat dilihat bahwa keamanan data nasabah juga menjadi poin penting dalam pelaksanaan layanan perbankan digital. Undang-Undang Perbankan sebagai dasar dari seluruh layanan dalam perbankan juga telah menetapkan dan memberikan perlindungan hukum atas data pribadi nasabah yaitu pada Pasal 29 ayat (4) Undang-Undang Perbankan yang menyatakan bahwa untuk kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan timbulnya risiko kerugian sehubungan dengan transaksi nasabah yang dilakukan melalui bank. Selanjutnya ketentuan mengenai kerahasiaan bank juga diatur dalam ketentuan Pasal 40 ayat (1), yaitu bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan

simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44, dan Pasal 44A.

Perlindungan hukum terhadap nasabah bank yang mengalami kebocoran data pribadi sangatlah relevan seiring meningkatnya digitalisasi layanan keuangan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi pijakan utama perlindungan hukum nasabah sebagai subjek data lembaga perbankan. Pasal 1 angka 2 Undang-Undang Perlindungan Data Pribadi, data pribadi diartikan sebagai setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya.,

Perlindungan hukum terhadap nasabah atas kebocoran data pribadi dalam penelitian ini dianalisis menggunakan teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon. Menurut Philipus M. Hadjon, perlindungan hukum terdiri atas perlindungan hukum preventif dan perlindungan hukum represif (Philipus M. Hadjon, 2015).

Perlindungan hukum preventif bertujuan mencegah terjadinya pelanggaran hukum melalui pembentukan regulasi dan sistem pengawasan, sedangkan perlindungan hukum represif bertujuan memberikan penyelesaian terhadap kerugian yang dialami oleh pihak yang dirugikan. Undang-Undang Perlindungan Data Pribadi memberikan dasar hukum yang kuat terhadap perlindungan data pribadi masyarakat dalam sistem elektronik. Dalam undang-undang tersebut, pengendali data pribadi memiliki kewajiban untuk menjaga keamanan dan kerahasiaan data pribadi yang berada dalam pengelolaannya. Bank sebagai pengendali data pribadi wajib memastikan bahwa sistem elektronik yang digunakan memiliki standar keamanan yang memadai guna melindungi data pribadi nasabah dari akses, penggunaan, maupun penyebaran yang tidak sah.

Perlindungan preventif diwujudkan melalui kewajiban pengendali data untuk mengadopsi prinsip kehati-hatian sejak awal pemrosesan data pribadi. Pasal 39 Undang-Undang Perlindungan Data Pribadi mengatur bahwa pengendali data wajib menerapkan prinsip perlindungan data pribadi, termasuk keabsahan pemrosesan, pembatasan tujuan, akurasi serta integritas dan kerahasiaan. Pada lembaga perbankan, prinsip ini mengharuskan bank untuk membangun sistem keamanan siber yang tidak hanya kuat secara teknis tetapi juga diperbaharui secara berkala guna menghadapi ancaman digital yang terus berkembang. Selain itu, bank perlu menetapkan kebijakan privasi yang transparan dan mudah diakses oleh nasabah serta menyediakan mekanisme pengawasan internal dan audit data yang efektif untuk mencegah penyalahgunaan data pribadi nasabah.

Perlindungan hukum preventif ini mencakup pula peningkatan kapasitas sumber daya manusia dalam mengelola data pribadi secara profesional dan etis, termasuk pelatihan rutin bagi karyawan mengenai protokol keamanan data. Bank juga harus selektif dalam menjalin kerja sama dengan pihak ketiga, seperti penyedia teknologi atau mitra bisnis yang memiliki akses terhadap data nasabah agar tetap mematuhi prinsip keamanan dan kerahasiaan sesuai standar Undang-Undang Perlindungan Data Pribadi.

Perlindungan hukum preventif terhadap nasabah juga diwujudkan melalui asas kerahasiaan bank. Asas kerahasiaan bank mewajibkan bank menjaga seluruh informasi mengenai nasabah dan simpanannya agar tidak disalahgunakan maupun diakses oleh pihak yang tidak berwenang. Dalam era digitalisasi perbankan, ruang lingkup asas kerahasiaan bank tidak hanya berkaitan dengan informasi simpanan nasabah secara konvensional, tetapi juga mencakup perlindungan terhadap data pribadi dan informasi elektronik nasabah yang tersimpan dalam sistem digital perbankan. Meskipun Indonesia telah memiliki berbagai regulasi mengenai perlindungan data pribadi dan rahasia bank, kasus gangguan sistem dan dugaan kebocoran data Bank Syariah Indonesia menunjukkan bahwa perlindungan hukum preventif terhadap data pribadi nasabah masih belum berjalan secara optimal. Hal tersebut terlihat dari masih adanya kelemahan sistem keamanan elektronik yang memungkinkan terjadinya gangguan sistem dan dugaan kebocoran data pribadi dalam layanan digital perbankan.

Perlindungan hukum preventif juga memperkuat hak-hak subjek data sebagaimana diatur dalam Pasal 12 dan Pasal 13 Undang-Undang Perlindungan Data Pribadi yang mencakup hak untuk mengakses, memperbaiki, membatasi, hingga menghapus data. Hak-hak ini memberikan kontrol aktif kepada nasabah atas informasi pribadinya dan memungkinkan mereka mengambil langkah korektif sebelum terjadi penyalahgunaan data lebih lanjut. Oleh karena itu, perlindungan preventif bukan hanya kewajiban normatif bagi bank melainkan instrumen strategis untuk menjaga kepercayaan nasabah dan reputasi institusi keuangan dalam jangka panjang.

Perlindungan hukum represif menyangkut hak nasabah untuk mendapatkan pemulihan hukum atas kerugian yang ditimbulkan. Pasal 58 Undang-Undang Perlindungan Data Pribadi menegaskan bahwa subjek data memiliki hak untuk mengajukan gugatan jika data pribadinya disalahgunakan atau dilanggar. Gugatan ini dapat ditempuh melalui jalur pengadilan perdata, sanksi administratif oleh otoritas pengawas maupun proses pidana bagi pelanggaran berat. Bank wajib membuktikan bahwa mereka telah melakukan langkah pengamanan sesuai standar, jika tidak maka tanggung jawab hukum dapat dijatuhkan.

Perlindungan hukum represif dalam lingkup kebocoran data pribadi menitikberatkan pada dua fungsi utama yaitu: memberikan keadilan dan pemulihan hak bagi korban (nasabah); menciptakan efek jera melalui sanksi yang proporsional terhadap pelaku termasuk institusi keuangan. Bentuk-bentuk kongkret perlindungan hukum represif yang tersedia dalam sistem hukum perbankan Indonesia sebagai berikut. Pertama, pengaduan kepada Otoritas Jasa Keuangan. Nasabah berhak mengajukan pengaduan kepada Otoritas Jasa Keuangan (OJK) jika mengalami pelanggaran data pribadi. Berdasarkan POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, Otoritas Jasa Keuangan memiliki wewenang menindaklanjuti laporan dan menjatuhkan sanksi administratif kepada lembaga keuangan yang terbukti lalai atau tidak memenuhi kewajiban perlindungan data. Kedua, Gugatan Perdata Perbuatan Melawan Hukum (PMH). Nasabah dapat mengajukan Gugatan Perbuatan

Melawan Hukum berdasarkan Pasal 1365 KUHPdata jika pelanggaran data pribadi menimbulkan kerugian yang nyata. Pertama, Sanksi Administratif dan Pidana. Bank yang melanggar ketentuan perlindungan data pribadi dapat dikenakan sanksi administratif berupa teguran tertulis, denda, penghentian kegiatan hingga pencabutan izin usaha sebagaimana diatur dalam Pasal 57 hingga Pasal 70 Undang-Undang Perlindungan Data Pribadi sedangkan untuk pelanggaran berat dapat dikenakan sanksi pidana maupun denda. Kedua, Pemberian Ganti Kerugian Kepada Korban. Pasal 12 ayat (1) Undang-Undang Perlindungan Data Pribadi menegaskan bahwa subjek data berhak menuntut dan menerima kompensasi secara langsung atas kerugian yang diderita akibat pelanggaran pemrosesan data pribadi.

Tanggung Jawab Hukum Bank Syariah Indonesia Terhadap Adanya Kebocoran Data Pribadi Nasabah

Tanggung jawab hukum pada dasarnya berkaitan dengan kewajiban seseorang atau badan hukum untuk menanggung akibat hukum dari suatu perbuatan yang dilakukan. Menurut Hans Kelsen, seseorang dikatakan bertanggung jawab secara hukum apabila terhadap dirinya dapat dikenakan sanksi atas perbuatan yang bertentangan dengan hukum (Hans Kelsen, 2019). Dengan demikian, pertanggungjawaban hukum muncul sebagai konsekuensi dari tidak dipenuhinya kewajiban hukum oleh subjek hukum yang bersangkutan. Dalam hubungan hukum antara bank dan nasabah, bank memiliki kewajiban hukum untuk menjaga keamanan sistem elektronik dan merahasiakan seluruh informasi mengenai nasabah yang berada dalam penguasaannya. Kewajiban tersebut lahir dari hubungan kepercayaan antara bank dan nasabah yang dikenal dengan asas kerahasiaan bank. Asas kerahasiaan bank merupakan prinsip fundamental dalam hukum perbankan yang mewajibkan bank untuk menjaga kerahasiaan data dan informasi nasabah. Kepercayaan masyarakat terhadap lembaga perbankan sangat bergantung pada kemampuan bank dalam menjaga keamanan dan kerahasiaan data pribadi nasabah. Oleh karena itu, kebocoran data pribadi nasabah pada dasarnya dapat dipandang sebagai bentuk pelanggaran terhadap kewajiban hukum bank dalam menerapkan asas kerahasiaan bank (Adrian Sutedi, 2022).

Kosep tanggung jawab pada hakikatnya memiliki keterkaitan dengan kewajiban hukum. Seorang ahli hukum bernama Austin memberikan pengertian mengenai kewajiban hukum. Menurutnya kewajiban hukum adalah diwajibkan melakukan atau tidak melakukan sesuatu atau ditempatkan dibawah kewajiban atau keharusan melakukan atau tidak melakukan adalah menjadi dapat dimintai pertanggungjawaban untuk suatu sanksi dalam hal tidak mematuhi suatu perintah (Jimly Asshiddiqie dan Ali Safa'at, n.d.).

Sebuah aturan hukum pada dasarnya berguna untuk mengatur dan memberikan kewajiban kepada subyek hukum dan subyek hukum tersebut diharuskan untuk melaksanakan kewajiban tersebut sebagai perintah dari aturan hukum (Ni Nyoman Ayu Ratih Pradnyani, 2020). Hans Kelsen juga memberikan pendapat mengenai konsep kewajiban hukum, menurut Hans Kelsen kewajiban hukum merupakan norma hukum

positif yang memerintahkan perilaku seorang individu dengan menetapkan sanksi atas perilaku yang sebaliknya (Hans Kelsen, 2019).

Kasus gangguan sistem dan dugaan kebocoran data yang dialami oleh Bank Syariah Indonesia tahun 2023 menunjukkan bahwa risiko kebocoran data pribadi dalam sektor perbankan digital merupakan persoalan hukum yang serius. Dugaan terbukanya data pribadi nasabah dan terganggunya sistem elektronik perbankan menimbulkan pertanyaan mengenai sejauh mana tanggung jawab hukum bank terhadap perlindungan data pribadi nasabah dalam sistem layanan digital perbankan.

Rahasia bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya. Hubungan kerahasiaan ini telah diatur dalam Pasal 40 Undang-Undang Perbankan yang menetapkan bahwa bank wajib merahasiakan keterangan nasabah penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam pasal 41, 41A, 42, 43, 44, dan 44A Undang-Undang Perbankan. Kewajiban bank untuk merahasiakan data mengenai nasabah penyimpan dan simpanannya menunjukkan bahwa Undang-Undang Perbankan memberikan perlindungan kepada nasabah berdasarkan prinsip kerahasiaan (Uswatun Hasanah, 2017).

Pada perspektif hukum perlindungan data pribadi, bank berkedudukan sebagai pengendali data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Sebagai pengendali data pribadi, bank memiliki kewajiban hukum untuk memastikan bahwa pemrosesan dan pengelolaan data pribadi dilakukan secara aman serta terlindungi dari akses, penggunaan, maupun penyebaran yang tidak sah.

Kedudukan bank sebagai pengendali data pribadi menunjukkan bahwa bank memiliki kontrol penuh terhadap sistem elektronik dan pengelolaan data nasabah. Oleh karena itu, apabila terjadi kebocoran data pribadi akibat gangguan sistem elektronik atau serangan siber, maka bank pada dasarnya tetap memiliki tanggung jawab hukum terhadap perlindungan data pribadi nasabah yang berada dalam pengelolaannya. Tanggung jawab bank terhadap perlindungan data pribadi nasabah tidak hanya bersifat administratif, tetapi juga merupakan bagian dari kewajiban hukum dalam pelaksanaan asas kerahasiaan bank dan prinsip kehati-hatian dalam kegiatan perbankan. Apabila bank gagal menjaga keamanan sistem elektronik sehingga menyebabkan kebocoran data pribadi nasabah, maka bank dapat dimintai pertanggungjawaban hukum atas kerugian yang dialami oleh nasabah.

Pertanggungjawaban pada dasarnya diberikan untuk membuktikan bahwa bank menjunjung tinggi asas kepercayaan. Kegiatan bank didasari oleh kepercayaan dari nasabah untuk menyimpan simpanannya di bank. Ketika nasabah telah mempercayakan simpanannya di bank, khususnya dalam perbankan digital, maka bank harus memaksimalkan segala upaya untuk tetap mempertahankan kepercayaan nasabah dengan memberikan pertanggungjawaban hukum kepada nasabah apabila terjadi kesalahan dalam sistemnya.

Pada hukum perdata, tanggung jawab hukum pada umumnya didasarkan pada adanya unsur kesalahan sebagaimana diatur dalam Pasal 1365 KUHPerdata mengenai perbuatan melawan hukum. Pasal tersebut menyatakan bahwa setiap perbuatan melawan hukum yang menimbulkan kerugian kepada orang lain mewajibkan pihak yang menimbulkan kerugian tersebut untuk mengganti kerugian yang timbul akibat perbuatannya.

Pada kasus Bank Syariah Indonesia, dugaan gangguan sistem dan kebocoran data pribadi dapat menunjukkan adanya kemungkinan kelemahan atau kegagalan sistem keamanan elektronik yang digunakan oleh bank. Sebagai lembaga yang mengelola sistem layanan digital dan data pribadi nasabah dalam jumlah besar, bank seharusnya memiliki sistem keamanan siber yang memadai untuk mencegah terjadinya serangan siber dan kebocoran data pribadi. Oleh karena itu, apabila terjadi kegagalan sistem keamanan yang menyebabkan data pribadi nasabah terbuka atau diakses oleh pihak yang tidak berwenang, maka kondisi tersebut dapat dipandang sebagai bentuk kelalaian dalam pelaksanaan kewajiban perlindungan data pribadi. Namun demikian, dalam praktiknya pembuktian unsur kesalahan dalam kasus kebocoran data pribadi seringkali sulit dilakukan.

Konsep *strict liability* menjadi relevan dalam kasus kebocoran data pribadi karena nasabah sebagai pihak yang dirugikan sering kali mengalami kesulitan untuk membuktikan adanya unsur kesalahan dari pihak bank dalam pengelolaan sistem keamanan data. Oleh karena itu, penting untuk dikaji apakah bank dapat dimintai pertanggungjawaban secara mutlak atas kebocoran data pribadi nasabah sebagai bentuk perlindungan hukum terhadap pihak yang dirugikan (Sodikin, 2022).

Nasabah sebagai pihak yang dirugikan tidak memiliki akses terhadap sistem internal dan teknologi keamanan yang digunakan oleh bank sehingga sulit membuktikan secara teknis adanya kelalaian atau kesalahan dari pihak bank. Di sisi lain, bank memiliki penguasaan penuh terhadap sistem elektronik dan informasi mengenai penyebab gangguan sistem maupun kebocoran data.

Tanggung jawab perdata dalam Pasal 60 Undang-Undang Perlindungan Data Pribadi memperkenalkan konsep *strict liability*, yang menetapkan bahwa pengendali data pribadi bertanggung jawab atas pemrosesan data pribadi kecuali dapat membuktikan bahwa kerugian tersebut terjadi bukan karena kesalahannya. Penerapan *strict liability*, fokus utama bukan terletak pada ada atau tidaknya kesalahan pelaku, melainkan pada adanya kerugian yang timbul akibat suatu kegiatan atau sistem yang berada dalam penguasaan pihak tertentu. Oleh karena itu, pihak yang menguasai dan memperoleh manfaat dari suatu kegiatan berkewajiban menanggung risiko hukum apabila kegiatan tersebut menimbulkan kerugian bagi pihak lain (Jimly Asshiddiqie dan Ali Safa'at, 2006).

Berdasarkan kondisi tersebut, menurut penulis konsep *strict liability* atau tanggung jawab mutlak lebih relevan diterapkan dalam kasus kebocoran data pribadi dalam sistem perbankan digital. Konsep *strict liability* merupakan bentuk pertanggungjawaban hukum yang tidak mensyaratkan adanya pembuktian unsur

kesalahan dari pihak yang bertanggung jawab. Dalam konsep ini, pihak yang mengelola kegiatan berisiko tinggi tetap bertanggung jawab terhadap kerugian yang timbul akibat kegiatan tersebut meskipun tidak dapat dibuktikan adanya unsur kesalahan secara langsung.

Strict liability merupakan bentuk pertanggungjawaban hukum yang tidak mensyaratkan adanya pembuktian unsur kesalahan dari pihak yang bertanggung jawab. Dalam konsep *strict liability*, seseorang atau badan hukum dapat dimintai pertanggungjawaban apabila kegiatannya menimbulkan kerugian bagi pihak lain, meskipun tidak dapat dibuktikan adanya unsur kesengajaan maupun kelalaian.

Konsep *strict liability* berkembang sebagai bentuk perlindungan hukum terhadap pihak yang dirugikan dalam kegiatan yang memiliki risiko tinggi terhadap keselamatan, keamanan, maupun hak-hak masyarakat. Prinsip ini bertujuan memberikan perlindungan yang lebih efektif kepada korban dengan cara meringankan beban pembuktian yang harus dilakukan oleh pihak yang dirugikan.

Penerapan konsep *strict liability* dalam kasus kebocoran data pribadi nasabah menjadi penting karena bank merupakan pihak yang memiliki kontrol penuh terhadap sistem elektronik dan memperoleh manfaat ekonomi dari penggunaan layanan digital perbankan. Nasabah hanya menggunakan layanan yang disediakan oleh bank dan tidak memiliki kendali terhadap sistem keamanan elektronik yang digunakan. Oleh karena itu, risiko kegagalan sistem keamanan seharusnya menjadi tanggung jawab bank sebagai penyelenggara layanan digital perbankan. Penerapan *strict liability* juga bertujuan memberikan perlindungan hukum yang lebih efektif terhadap nasabah sebagai pihak yang posisinya lebih lemah dalam hubungan hukum dengan bank.

Konsep *strict liability* menjadi sangat relevan dalam kasus kebocoran data pribadi nasabah perbankan. Dalam sistem perbankan digital, seluruh penguasaan dan pengendalian sistem elektronik berada di bawah kewenangan bank sebagai penyelenggara layanan jasa keuangan. Bank memiliki kendali penuh terhadap server, sistem keamanan data, pengelolaan informasi nasabah, serta infrastruktur teknologi yang digunakan dalam operasional layanan perbankan digital.

Penerapan *strict liability* juga sejalan dengan prinsip kehati-hatian dan asas kepercayaan dalam sektor perbankan. Bank sebagai lembaga keuangan memiliki kewajiban hukum untuk menjaga keamanan dan kerahasiaan data pribadi nasabah secara optimal. Dengan demikian, apabila terjadi kebocoran data pribadi nasabah, maka bank pada prinsipnya tetap harus bertanggung jawab atas kerugian yang dialami nasabah sebagai konsekuensi dari kewajiban perlindungan data pribadi dan penerapan asas kerahasiaan bank.

Prinsip *strict liability* atau tanggung jawab mutlak itu mewajibkan pelaku usaha atau korporasi dalam hal ini perbankan wajib memberikan ganti rugi jika ada kerugian dan hubungan kausalitas tanpa perlu membuktikan ada kesalahan dari pihak perbankan sehingga korban tidak dibebani membuktikan unsur kesalahan, cukup membuktikan

kerugian dan sebab-akibat (*no liability without fault*). Akan tetapi memang prinsip strict liability ini pada prakteknya belum bisa dilaksanakan.

Hukum perdata Indonesia secara umum menganut *liability based on fault*. Ini secara eksplisit sebagaimana dimaksud dalam Pasal 1365 KUHPerdata yang menjelaskan: "*tiap perbuatan melanggar hukum, yang membawa kerugian kepada orang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian.*" Dan implisitnya sebagaimana tertuang dalam Peraturan Otoritas Jasa Keuangan yaitu POJK 1/POJK.07/2013 yang mewajibkan prinsip keseimbangan, keadilan, kewajaran dalam perjanjian baku. Jadi beban pembuktian kesalahan masih di nasabah kecuali bank lalai.

Konsep *strict liability* belum diakomodir dalam hukum perbankan di Indonesia sehingga beban pembuktian dilimpahkan kepada nasabah bukan kepada lembaga perbankan secara mutlak. Hal ini jelas merugikan karena tidak memberikan perlindungan terhadap nasabah yang dirugikan karena upaya penegakan hukum yang selama ini berlangsung dengan *based on liability* misal dengan melakukan Gugatan Perbuatan Melawan Hukum sebagaimana dimaksud Pasal 1365 KUHPerdata dengan beban pembuktian ada pada nasabah pada pelaksanaannya dianggap masih sulit, lama dan berbiaya mahal hal ini jelas bertolak belakang dengan asas hukum peradilan cepat, sederhana dan biaya ringan. Sehingga menurut hemat penulis jika dalam konsep *based on liability* perlindungan hukum terhadap nasabah kurang maka penerapan konsep *strict liability* (pertanggung jawaban mutlak) menjadi langkah solusi yang terbaik.

Kesimpulan

Berdasarkan pembahasan yang telah diuraikan di atas dan untuk menjawab pokok permasalahan yang diangkat dalam penelitian ini, maka kesimpulan dari penelitian ini adalah sebagai berikut. Perlindungan hukum terhadap nasabah atas kebocoran data pribadi dalam sistem perbankan digital pada dasarnya telah diatur dalam berbagai ketentuan peraturan perundang-undangan di Indonesia. Perlindungan data pribadi dalam sektor perbankan harus dilakukan secara lebih komprehensif melalui penguatan regulasi, pengawasan, dan keamanan sistem elektronik. Namun demikian hasil penelitian menunjukkan bahwa perlindungan hukum terhadap nasabah dalam praktiknya masih belum berjalan secara optimal.

Kasus gangguan sistem dan dugaan kebocoran data Bank Syariah Indonesia Tahun 2023 menunjukkan bahwa kebocoran data pribadi nasabah dapat dipandang sebagai bentuk gangguan terhadap pelaksanaan asas kerahasiaan bank apabila menyebabkan data pribadi nasabah dapat diakses atau disalahgunakan oleh pihak yang tidak berwenang. Konsep *strict liability* lebih relevan diterapkan dalam kasus kebocoran data pribadi dalam sistem perbankan digital karena bank memiliki kontrol penuh terhadap sistem elektronik dan pengelolaan data pribadi nasabah, sedangkan nasabah berada pada posisi yang lebih lemah dalam hal penguasaan teknologi informasi dan pembuktian kesalahan bank.

Pihak bank diharapkan untuk meningkatkan sistem keamanan siber dan perlindungan data pribadi nasabah melalui pembaruan sistem teknologi informasi, peningkatan standar keamanan digital, audit keamanan sistem elektronik secara berkala, serta peningkatan kualitas sumber daya manusia dalam bidang keamanan siber. Pihak nasabah diharapkan dapat lebih berhati-hati dalam mengakses segala hal yang berkaitan dengan transaksi elektronik serta menambah wawasan mengenai keamanan data pribadi dan informasi mengenai bank yang digunakan. Dengan adanya penguatan regulasi, peningkatan keamanan sistem elektronik, pengawasan yang efektif, serta peningkatan kesadaran nasabah terhadap perlindungan data pribadi, maka perlindungan hukum terhadap nasabah dalam sistem perbankan digital di Indonesia diharapkan dapat terlaksana secara lebih optimal dan mampu memberikan kepastian hukum serta rasa aman bagi nasabah sebagai pengguna layanan digital perbankan. Selain itu penerapan *strict liability* sebaiknya di normakan dalam undang-undang guna menciptakan perlindungan hukum korban atas kebocoran data pribadi oleh perbankan.

Referensi

- Abd. Shomad dan Trisadini P. Usanti. (2016). *Hukum Perbankan*. Kencana.
- Adrian Sutedi. (2022). Prinsip Kerahasiaan Bank dan Perlindungan Nasabah. *Jurnal Hukum Bisnis*, 38(1), 45–47.
- Budi Agus Riswandi. (2023). Implikasi UU Perlindungan Data Pribadi terhadap Sektor Jasa Keuangan. *Jurnal Legislasi Indonesia*, 20(03), 389–392.
- CST Kansil. (2011). *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*. Balai Pustaka.
- Hans Kelsen. (2019). *Teori Hukum Murni: Dasar-Dasar Ilmu Hukum Normatif*. Nusamedia.
- Iqbal Hasan. (2022). *Metodologi Penelitian dan Aplikasinya*. Ghalia Indonesia.
- Jimly Asshiddiqie dan Ali Safa'at. (n.d.). *Teori Hans Kelsen tentang Hukum*. Sekretariat Jenderal & Kepaniteraan Mahkamah Konstitusi RI.
- Kamus Besar Bahasa Indonesia*. (n.d.). Retrieved August 11, 2026, from <https://kbbi.web.id/>
- Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram University Press.
- Muhammad Faisal Aziz dkk. (2025). Perlindungan Hukum terhadap Nasabah atas Penyalahgunaan Data Pribadi oleh Pihak Bank di Era Digitalisasi Perbankan. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(6).
- Muhammad Syafii Antonio. (2019). *Bank Syariah Dari Teori ke Praktek*. Gema Insani.
- Ni Nyoman Ayu Ratih Pradnyani. (2020). *Tanggung Jawab Hukum dalam Penolakan Pasien Janiman Kesehatan Nasional*. Scopindo.
- Philipus M. Hadjon. (2015). *Perlindungan Hukum bagi Rakyat di Indonesia*. Bina Ilmu.
- Rika Ratna Sembiring. (2023). Perlindungan Data Pribadi Nasabah Perbankan di Era Digital. *Jurnal Hukum IUS QUIA IUSTUM*, 30(2).
- Satjipto Rahardjo. (2009). *Hukum dan Masyarakat*. Angkasa.
- Sinta Dewi Rosadi. (2023). Tanggung Jawab Pengendali Data dalam Kebocoran Data Pribadi. *Jurnal Hukum & Pembangunan*, 53(1), 112–115.
- Sodikin. (2022). Perkembangan Konsep Strict Liability Sebagai Pertanggungjawaban Perdata Dalam Sengketa Lingkungan Di Era Globalisasi. *Al-Qisth Law Review*, 5(2).

Sudikno Mertokusumo. (2010). *Mengenal Hukum Suatu Pengantar* . Liberty.
Uswatun Hasanah. (2017). *Hukum Perbankan* . Setara Press.