

Pertanggungjawaban Perbankan Dalam Melindungi Data Pribadi Nasabah Akibat Peretasan Studi Kasus Bank Syariah Indonesia

Trianda Lestari

Universitas Maritim Raja Ali Haji

triandalestari9@gmail.com

Syahrando Muhti

Universitas Maritim Raja Ali Haji

syahrandomuhti08@gmail.com

Reky Yuliansyah

Universitas Maritim Raja Ali Haji

Yuliansyahreky11@gmail.com

Alamat: Jl. Raya Dompok, Dompok, Kec. Bukit Bestari, Kota Tanjung Pinang, Kepulauan Riau 29115

Korespondensi penulis: triandalestari9@gmail.com

Abstract. *Abstract. BSI is one of the banks that experienced hacking and attacks from irresponsible parties. Lockbit threatened BSI to immediately contact him to carry out negotiations regarding 1.5 TB of customer data which was threatened with being disseminated if BSI did not fulfill its request by the specified time limit. given. In the end, this happened because the given time limit had passed, there was a lockbit post showing a link connected to banking data. This case has certainly become the center of attention, because BSI is still reluctant to provide further information regarding customer data leaks and personal data protection has not been provided. This research method uses a normative legal method which refers to statutory regulations and related sources. The legal theory used is the theory of legal certainty, to see how certain banks provide responsibility for protecting customers' personal data as regulated in banking law. So researchers can also find the title in the article entitled Banking Responsibility in protecting personal data of bank customers due to hacking BSI case study*

Keywords: Protection, Banking, Hacking, Liability

Abstrak. BSI menjadi salah satu bank yang mengalami peretasan dan serangan dari pihak yang tak bertanggungjawab, Lockbit yang memberikan ancaman kepada BSI agar untuk segera menghubunginya untuk bernegosiasasi terkait 1,5 Tb data nasabah yang menjadi ancaman akan disebarluaskan apabila pihak BSI tidak memenuhi permintaannya hingga batas waktu yang diberikan. Pada akhirnya hal tersebut terjadi karena sudah melewati batas waktu yang diberikan, terdapat postingan lockbit yang memperlihatkan link yang terhubung dengan data-data perbankan. Kasus ini tentu menjadi pusat perhatian, karena pihak BSI masih saja enggan untuk memberikan informasi lanjut terkait kebocoran data nasabah hingga perlindungan data pribadi belum mendapatkan perlindungan. Metode penelitian ini menggunakan metode hukum normative yang mengacu pada peraturan perundang-undangan dan sumber yang terkait. Teori hukum yang digunakan adalah teori kepastian hukum, untuk melihat bagaimana kepastian pihak perbankan dalam memberikan tanggungjawab dalam perlindungan data pribadi nasabah sebagaimana yang sudah diatur dalam undang-undang perbankan. Hingga dapat pula peneliti temukan judul dalam penulisan ini yang berjudul Pertanggungjawaban Perbankan Dalam Melindungi Data Pribadi Nasabah Akibat Peretasan studi Kasus BSI

Kata kunci: Perlindungan, Perbankan, Peretasan, Pertanggungjawaban.

LATAR BELAKANG

Bank Syariah Indonesia (BSI) didirikan tepat pada tanggal 1 Februari 2021 yang merupakan hasil dari bank BRI Syariah TBK, Bank Syariah Mandiri dan BNI Syariah. Terdapat

komposisi beberapa pemegang saham BSI yaitu Bank Mandiri 59,83% BNI 24,85%, dan BRI 17,25%, serta sisanya merupakan magang saham dibawah 5%. Dengan hal itu BSI digadang menjadi bank yang besar diindonesia bahkan BSI menduduki 10 besar bank syariah tingkat dunia. Sebagaimana akhir-akhir ini baru saja terjadi peretasan/kebocoran data pribadai nasabah bank pada BSI yang cukup menghebohkan dunia perbankan.

Tepat pada tanggal 8 mei, layanan mobile banking dan ATM Bank syariah Indonesia sempat terganggu selama sepekan. Pada saat itu menduga jika hanya terjadi pemeliharaan sistem sehingga tidak bisa diakses. Akan tetapi tepat pada tanggal 14 mei 2023 terungkap fakta yang cukup mengejutka bahwa yang terjadi pada gangguan tersebut disebabkan oleh adanya serangan *ransmware*. *Ransmware* merupakan sejumlah serangan dari hacker, ransmware itu sendiri merupakan jenis perangkat lunak yang berbahaya yang dapat mengunci dan menghambat akses ke sistem computer korban dengan mengenskripsi data untuk meminta uang tebusan.

Pelaku peretasan tersebut memberikan waktu kepada pihak bank selama 72 jam untuk menghubungi mereka, dan memberikan ancaman kepada pihak bank mereka akan meruntuhka reputasi bank secera terseluruh apabila keinginannya tidak terpenuhi. Alih alih menghirukan hacker, pihak manajemen bank malah mendalilkan bahwa layanan BSI sedang dalam masa *maintenance*. Hingga akhirnya hacker berhasil menginfeksi sistem perbankan BUMN tersebut serta menyandera data nasabah bank.

Kebocoran data pribadi nasabah bank merupakan hal yang sangat serius dalam dunia perbankan, bagaimana tidak dengan hidup di era digital yang semakin maju dan canggih maka berdampak timbulnya tindakan kejahatan pada sektor perbankan saat ini. Terdapat beberapa informasi data nasabah seperti nomor rekening, informasi kartu kredit, data identitas, serta detail keungan yang cukup membuat kerugian sangat besar. Adanya tindakan semacam ini membuat dampak yang cukup besar pada dunia perbankan bukan hanya masalah pelanggaran keamanan data. Pencurian, dan penyalahgunaan finansial akan tetapi dapat menimbulkan ketidakpercayaan nasabah terhadap institusi perbankan serta kerugian reputasi yang sangat signifikan.

Teguh Aprianto selaku pengamat siber dalam akun tweeternya mengungkapkan bahwasannya data BSI sudah resmi dibocorkan secara bertahap oleh kelompok hacker dengan estimasi total 8.133 file yang akan dibocorkan secara keseluruhan, lanjutnya lagi ia menjelaskan bahwa sebanyak data pribadi sebesar 24,437 karyawan BSI dan

juga dokumen internal sudah masuk ke lilist yang ternyata sudah dibocorkan dari awal. Terdapat beberapa data yang telah bocor yaitu nomor hp, email, alamat, nomor ID Karyawan, status karyawan, informasi jabatan, informasi penempatan karyawan, informasi manajer yang bertanggung jawab, kebocoran data juga berimbas kepada mantan karyawan.

Pada keterangan ransomware lockbit 3.0. menjelaskan seragan tersebut sudah dilakukan selama dua bulan. Bahwasannya mereka mengaku sebagai actor dibalik gangguan layanan BSI yang sudah terjadi pada 8 mei tahun 2023. Menurut dari keterangan hacker yang mengakui bahwa telah mencuri 15 juta catatan pelanggaran, serta informasi karyawan dan sekitar 1,5TB data internal ransomware lockbit 3.0. yang pada akhirnya mereka mengancam akan memberikan semua data di situs gelap jika negoisasi gagal.

Pada kemudian komisi VI DPR RI Amin AK memerintahkan agar kementerian BUMN bertanggung jawab atas dugaan kebocoran 15 juta data nasabah dibank syariah Indonesia. Dari keterangannya bahwa hal ini perlu diambil tindakan oleh pemerintah agar melindungi data nasabah. Tuturnya lagi kementerian BUMN yang bertugas mengawasi bank-bank BUMN tidak bisa lepas tangan begitu saja dikarenakan kasus peretasan semacam ini sering kali terjadi. Dari hal seperti ini sudah terlihat bahwa sistem peratahanan sober bank-bank diindonesia kurang kuat.

Sebagaimana yang sudah terjadi pada dunia perbankan sebelum-sebelumnya seperti yang terjadi pada tahun 2021 kasus peretasan Bank Jatim dan BRI Life yang juga menjadi korban kebocoran dan peretasan data pribadi nasabah bocor diinternet. Serta kasus yang serupa terjadi pada tahun 2022 Bank Indonseia mengaku terkena serangan ransomware. Kasus semacam ini sangat cukup sering terjadi pada sekor perbankan yang cukup dirugikan adalah para nasabah yang datanya mengalami kebocoran, perlunya tindakan tegas atas perlindungan data pribadi nasabah sebagaimana

Dalam prinsip kepercayaan bahwa mengharuskan semua pihak dalam suatu transaksi atau hubungan hukum untuk bertindak dengan itikad baik dan jujur. Prinsip ini sangat relehvan dengan konteks perlindungan data nasabah. Bank memiliki tanggung jawab hukum dan moral untuk melindungi data pribadi nasabah mereka. Jika terjadi kebocoran data, prinsip kepercayaan mewajibkan bank untuk segera mengambil tindakan untuk memperbaiki kerugian. Serta bank wajib untuk memiliki sistem keamanan yang kuat untuk mencegah peretasan dan mempersiapkan rencana penanggulangan jika peretasan terjadi.

Dari kasus kebocoran data pribadi nasabah tersebut lalu bagaimanakah bentuk perlindungannya dan siapa yang bertanggung jawab atas masalah tersebut, maka penulis akan melanjutkannya dalam penelitian ini yang berjudul Perlindungan Data Pribadi nasabah Bank BSI yang mengalami kebocoran Data

Dari kasus peretasan tersebut diharapkan adanya perbaikan yang cukup dalam mencegah dan menangani data pribadi. Dengan adanya penegakan ketat terhadap kebijakan keamanan data, penerapan teknologi yang aman, dan transparansi yang tinggi dalam mengatasi insiden kebocoran, sektor perbankan harus dapat memulihkan kepercayaan nasabah dan juga melindungi segala privasi data nasabah, diharapkan adanya kebocoran data pada sektor perbankan dapat ditekan sejauh mungkin sehingga nasabah merasa lebih dan aman nyaman dan terlindungi dalam menggunakan layanan perbankan

KAJIAN TEORITIS

Penelitian ini menggunakan teori kepastian hukum, yang dimana mengacu pada ketentuan hukum yang jelas. Teori kepastian hukum menekankan pentingnya adanya ketentuan hukum yang jelas dan terperinci terkait perlindungan data pribadi. Dengan melihat apakah terdapat ketentuan hukum yang memadai dan spesifik yang mengatur perlindungan data pribadi nasabah bank. Serta mengacu pada responsibilitas dan akuntabilitas teori kepastian hukum juga menuntut adanya responsibilitas dan akuntabilitas dari pihak-pihak yang terlibat dalam perlindungan data pribadi nasabah bank. Hal ini untuk melihat sejauh mana tanggung jawab bank dalam melindungi data pribadi nasabah dan bagaimana mereka bertanggung jawab atas kebocoran data yang terjadi.

METODE PENELITIAN

Penelitian ini menggunakan penelitian hukum normative yang hanya mengacu pada sumber-sumber informasi dari buku, jurnal, artikel dan maupun internet serta yang terdapat dalam peraturan perundang undangan. Teknik pengumpulan data menggunakan teknik studi kepustakaan

HASIL DAN PEMBAHASAN

Pada kegiatan perbankan di Indonesia sebagaimana yang berdasarkan demokrasi ekonomi hal ini mendasarkan pada prinsip kehati-hatian. Prinsip kehati-hatian merupakan kehasan dari

dunia perbankan, yang harus sesuai dengan ideology panacasila serta tujuan Negara yang tercantum dalam undang-undang dasar 1945. Perbankan yang didasarkan demokrasi ekonomi mempunyai arti bahwa masyarakat lebih memegang peranan aktif dalam perbankan. Pemerintah turut bertanggung jawab dalam memberikan pengarahannya serta bimbingan dalam pertumbuhan perbankan sektor ekonomi dan menciptakan pertumbuhan yang baik dalam dunia usaha.

Dalam pasal 1 ayat (3) UUD 1945 ditegaskan bahwa Indonesia ialah Negara hukum, sebagaimana pada kegiatan perekonomian pada perbankan di Indonesia pada dasarnya memegang prinsip hukum dan tidak bertentangan dengan hukum. Serta dalam pasal 1 angka (28) UU Nomor 10 Tahun 1998 tentang perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang perbankan, Rahasia bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpanan dan simpanannya. Sebagaimana penjelasan tersebut yang juga mencakup kerahasiaan pribadi data nasabah bank yang wajib dilindungi dan dirahasiakan hal ini yang juga sudah dimuat dalam pasal 40 ayat (1) UU perbankan yang menyatakan bahwa bank tersebut wajib merahasiakan keterangan mengenai nasabah penyimpanan dan simpanannya.

Dalam pasal 26 ayat (1) UU Nomor 1 Tahun 2008 Tentang informasi dan transaksi elektronik menjelaskan bahwa kecuali ditentukan lain oleh peraturan perundang-undangan Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan Sebagaimana dalam peraturan Bank Indonesia Nomor 7/PBI/2005 yang merupakan landasan dari pasal 26 ayat (1) UU No 11 Tahun 2008 tentang informasi dan transaksi elektronik. yang bertujuan agar nasabah tersebut mengetahui resiko pada produk bank yang ditawarkan dan agar perlindungan data atas data pribadi nasabah bank terpenuhi.

Merujuk kasus BSI yang mengalami kebocoran data pribadi maka pihak BSI wajib memberikan perlindungan data pribadi nasabah bank. Namun dengan mengingat kembali Indonesia memiliki undang-undang perlindungan data pribadi yang disahkan pada September tahun lalu, dengan mengacu pada regulasi tersebut menurut Pratama Persadha apabila BSI terbukti bersalah maka sanksi administrative diterapkan sesuai pada pasal 57 UU PDP. Namun sayangnya UU PDP baru akan berlaku pada oktober 2024 selain itu otoritas yang bertugas menyelenggarakan perlindungan data pribadi belum dibentuk.

BSI yang sebagaimana terus tidak mengakui atas adanya kebocoran data serta BSI enggan menyampaikan pemberitahuan secara tertulis kepada subjek data pribadi terkait serangan siber yang berdampak pada peretasan data nasabah, Sebaliknya BSI justru mengklaim lumpuhnya sistem dan pelayanan bank disebabkan oleh proses maintenance. Seorang pakar keamanan yaitu Alfons Tanujaya mengatakan bahwa jika bank mengalami gangguan selama lebih kurang dari empat jam, hal ini memang dikarenakan gangguan sistem inti yaitu adanya serangan ransomware. Namun pada nyatanya meski banyak media masa yang berusaha untuk mengulik informasi dari BSI mengenai serangan ransomware ini. BSI tidak menanggapi lebih. Dari masalah itulah sampai saat ini perlindungan data pribadi nasabah bank belum mendapatkan perhatian yang memadai dalam sistem perbankan nasional. Maka Dengan Perlindungan data pribadi, pengendali PDP yang jelas tidak melaksanakan perlindungan data pribadi dengan baik maka dapat dituntut di pengadilan melalui proses iinvestigasi yang dilakukan oleh lembaga yang disebut LPDP.

1. Penanganan data pribadi sesuai regulasi atas kebocoran data BSI

Lembaga perlindungan data pribadi yang akan menangani insiden kebocoran data pribadi. Namun lembaga tersebut belum terbentuk, Mekanisme penegakan hukum dalam UU PDP belum dapat berjalan dengan baik dan jelas. Denngan adanya kegagalan perlindungan data pribadi BSI yang sebagai pengendali wajib melakukan berbagai upaya dengan mengacu pada hal-hal berikut

a) BSI wajib memberikan notifikasi

BSI harus memberikan notifikasi/informasi kepada nasabah atau subjek data paling lama tiga kali duapuluh empat jam termasuk kepada masyarakat mengingat insidin ini terkait dengan layananan public, hal ini sebagaimana dengan mengacu pada pasal 46 UU 27/2022. Namun masalahnya dalam peraturan ini tidak jelas diatur mengenai waktu tersebut.

Namun mengulik pada Permenkominfo 20/2016 dengan menghitung waktu/priode pada setelah terjadinya insiden Hal ini PJOK PTI mewajibkan diberikan notifikasi awal paling lama satu kali selama dua puluh empat jam serta melaporkan insiden TI tersebut selama kurang lebih lima hari kerja setelah insiden pada Otoritas Jasa Keuangan

b). Melakukan pemulihan yang mengacu pada UU 27/2022 PP 71/2019

Dengan mengacu pada UU Nomor 27/2022 pp 71/2019. Permenkominfo 20/2016. Serta PJOK PTI yang harus mewajibkan Ban/Lemmbaga keungan untuk memiliki rencana pemulihan bencana hal ini agar memastikan kelangsungan operasional bank tetap berjalan

selama insiden.. BSI wajib mengawasi rencana penanggulangan data serta pemulihan dengan *Business continuity plan crisis management plan*, / kebijakan/ rencana bank lainnya yang terkait.

Dengan berpijak pada ketentuan pasal 4 ayat (2) UU 27/2022 data keuangan pribadi merupakan bagian dari data yang spesifik. Dengan begitu hal ini sangat memerlukan perlindungan yang sangat signifikan termasuk juga saat terjadi kegagalan dalam perlindungan data seta sangat memerlukan langkah-langkah dalam penanganannya. Untuk memastikan perlindungan tersebut daalm pemenuhan hak-hak subjek data tersebut elsam memerintahkan pihak terkait untuk ertindak melakukan langkah terebut. Khususnya BSI yang harus memberikan notifikasi perihal kegagalan perlindungan data pribadi kepada nasabah tanpa penundaaan yang tidak perlu dalam bentuk secara tertulis

Serta juga dalam upaya penanganan dan pemulihan atas kegagalan tersebut sebagaimana hal ini sudah diatur dalam pasal 46 ayat (2) UU 27/2022. Dan juga BSI wajib memberikan informasi terkait kontak informasii yang dapat dihubungi oleh subjek data. Dan juga langkah-langkah mitigasi yang dilakukan oleh nasabah hal ini dapat memperkecil resiko akibat kebocoran data.

c). OJK perlu Mengevaluasi

OJK harus mengevaluasi terhadap langkah mitigasi dan memastikan pemutakhiran rencana pemulihan BSI yang telah sesuai pada POJK PTI. Dan serta mengaudit keseluruhan rencana mitigasi dan pemulihan pada sistem teknologi informasi dari industry perbankan.

d). Pengawasan Kominfo

Melalui kewenangan dan pengawasan Kominfo segera menginvestigasi dan menyelesaikan kasus secara akuntabek, dalam mengidentiffikasi penyebab kegagalan perlindungan data pribadi, Serta mengidentifikasi kerugian pada pengendali, prosesor, dan subjek data dan juga memberikan informasi terkait hasil investigasi secara akutabel. Dan juga memastika pemulihan terhadp hak-hak subjek data

e). Melalui BSSN

Badan Siber dan sandi Negara harus segera memantau dan mengidentifikasi insiden keamanan siber yang dialami BSI. Hal ini untuk dapat didentifikasi sumber serangakerentanan sistem keamanan yang ini memungkinkan terjadinya serangan dan n juga BSSN harus

memastikan adanya audit keamanan secara berkala, termasuk juga penerapan keamanan yang kuat bagi keseluruhan industry perbankan dan keuangan

2. Mekanisme pertanggungjawaban BSI

Terhadap kebocoran data BSI sampai saat ini belum juga mendapatkan perhatian lebih dari BSI dalam pemberian perlindungan data pribadi seharusnya BSI memberikan tanggung jawab yang penuh. Berdasarkan asas/prinsip hukum perbankan yaitu prinsip secrecy perbankan. Bank wajib melindungi data nasabah dan berarti bank wajib memiliki tanggung jawab untuk melindungi data serta informasi nasabah dari kebocoran. Terdapat adanya prinsip kerahasiaan bank tidak bersifat mutlak, yang artinya terdapat beberapa masalah dimana bank sendiri dapat membuka data dan informasi nasabah akan tetapi hal ini ada aturan dan prosedur yang ketat

Jika terjadi kebocoran data BSI harus bertanggung jawab dan melakukan langkah-langkah yang bertujuan untuk memperbaiki dan mencegah kejadian tersebut dimasa sekarang dan masa yang akan datang. Otoritas Jasa keuangan telah mengeluarkan peraturan No 12/PJOK.03/2018 yang dimana hal ini berkaitan dengan penyelenggaraan layanan perbankan digital oleh bank umum. Peraturan ini untuk memastikan bank penyelenggara memiliki infrastruktur dan manajemen teknologi informasi yang memadai serta wajib menerapkan prinsip perlindungan nasabah.

Berpijak pada pasal 4 UU No.8 Tahun 1999 tentang perlindungan konsumen, nasabah atau konsumen berhak untuk dilindungi, pihak pengelola atau manajemen bank wajib melindungi dan bertanggung jawab. Pada hal ini sebelum berlakunya UU PDP dalam pengaturan data pribadi nasabah lembaga perbankan telah diatur dalam undang-undang mengenai perbankan yaitu undang-undang Nomor 10 Tahun 1998 tentang perubahan atas UU No 7/1992 tentang perbankan. Sebagaimana telah diubah terakhir kali dengan UU No 4 Tahun 2023 tentang pengembangan dan penguatan sektor keuangan.

Dalam Undang-Undang perbankan mengatur kewajiban bank untuk merahasiakan terkait nasabah penyimpanan atau simpanan hal ini sejalan dengan Otoritas Jasa Keuangann mengeluarkan surat nomor 14/SEOJK.07/2014 tentang kerahasiaan dan keamanan data dan informasi pribadi konsumen. Dalam keterangan edaran tersebut sebagaimana telah diatur bahwa pelaku usaha jasa keuangan (PUJK). Pada khususnya BSI diwajibkan untuk melindungi data dan atau informasi pribadi konsumen kepada pihak ketiga. Disamping itu terdapat beberapa Hak nasabah dalam UU PDP

- a) Hak atas informasi pihak yang memberikan data

- b) Kewajiban pengendali data dalam pemrosesan data pribadi
- c) Informasi yang harus disampaikan oleh pengendali data
- d) Persetujuan legalitasnya jika pemberi data setuju
- e) Bentuk dan syarat persetujuan
- f) Tidak semua persetujuan dianggap sebagai persetujuan
- g) Adanya sanksi

Maka dengan hal ini jika terjadinya kebocoran data pihak bank memiliki kewajiban memberitahukan kebocoran data nasabah, namun apabila perusahaan tidak memberitahukan maka akan berdampak negative kepada nasabah sebagaimana pada kasus BSI. Dalam pasal 12 ayat (1) UU PDP menjelaskan bahwa apabila terjadi kegagalan dalam perlindungan data pribadi, subjek, termasuk nasabah, berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tersebut.

Terdapat beberapa bentuk pertanggungjawaban BSI terhadap kebocoran data nasabah berdasarkan UUPK yang tidak terlepas dari prinsip tanggung jawab perdata dan dalam Peraturan Bank Indonesia No 22/20/PBI/2020. Yaitu

- a) Prinsip tanggung jawab berdasarkan unsur kesalahan
Prinsip ini sebagaimana sejalan dengan pasal 1365 KUHPerdata yang menyatakan bahwa *“Tiap perbuatan melanggar hukum,, yang membawa kerugian kepada seseorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu mengganti kerugian tersebut”*
- b) Prinsip tanggungjawab mutlak
Prinsip tanggungjawab mutlak atau sering kali diartikan sebagai prinsip tanggungjawab absolut. Prinsip tersebut menetapkan bahwa kesalahan tidak sebagai factor yang menentukan
- c) Kesetaraan dan perlakuan yang adil.
Setiap nasabah harus mendapatkan perlakuan yang sama dan adil
- d) Keterbukaan dan transparansi
Bank harus transparan dalam menyampaikan informasi terkait produk dari layanan mereka
- e) Perlindungan data dan atau informasi konsumen.
Bank harus melindungi data dan informasi pribadi nasabah dari penyalahgunaan
- f) Penanganan dan penyelesaian pengaduan yang efektif.
Bank harus memiliki mekanisme penanganan dan penyelesaian pengaduan yang efektif

Dalam kasus kebocoran data BSI hemat peneliti hal ini akibat dari adanya perbuatan melawan hukum pasal 1365 KUHperdata. Maka pihak BSI harus melakukan ganti rugi dan mengembalikan data tersebut atas kelalaian BSI, jika berpijak pada pasal 1365 bahwasannya atas perbuatan melawan hukum maka pihak nasabah dapat menuntut pada BSI dengan menggugat di PN yang sesuai dengan kompetensi absolut dan kompetensi relative pasal 113 HIR.

Dari kasus peretasan tersebut diharapkan adanya perbaikan yang cukup dalam mencegah dan menangani data pribadi. Dengan adanya penegakan ketat terhadap kebijakan keamanan data, penerapan teknologi yang aman, dan transparansi yang tinggi dalam mengatasi insiden kebocoran, sektor perbankan harus dapat memulihkan kepercayaan nasabah dan juga melindungi segala privasi data nasabah, diharapkan adanya kebocoran data pada sektor perbankan dapat ditekan sejauh mungkin sehingga nasabah merasa lebih dan aman nyaman dan terlindungi dalam menggunakan layanan perbankan

KESIMPULAN DAN SARAN

Perlindungan data pribadi nasabah bank BSI sampai saat ini belum mendapatkan perhatian lebih, pihak BSI masih saja mengelak dan beralasan saat dimintai keterangan terkait kebocoran data nasabah, hal ini tentu menjadi perhatian lebih dikarenakan terdapat beberapa data nasabah bank yang mengalami kebocoran peretasan yang mengalami kerugian bagi nasabah tersebut, dari kasus tersebut maka melihat ketentuan pasal 4 UU No.8 Tahun 1999 tentang perlindungan konsumen, nasabah atau konsumen berhak untuk dilindungi, pihak pengelola atau manajemen bank wajib melindungi dan bertanggung jawab, peraturan No 12/PJOK.03/2018 yang dimana hal ini berkaitan dengan penyelenggaraan layanan perbankan digital oleh bank umum. Peraturan ini untuk memastikan bank penyelenggara memiliki infrastruktur dan manajemen teknologi informasi yang memadai serta wajib menerapkan prinsip perlindungan nasabah. Namun apabila pihak nasabah tidak mendapatkan perlindungan maka sesuai ketentuan Dalam pasal 12 ayat (1) UU PDP menjelaskan bahwa apabila terjadi kegagalan dalam perlindungan data pribadi, subjek, termasuk nasabah, berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tersebut. BSI perlu lebih baik lagi dalam menangani masalah tersebut dan jika terjadi kebocoran data sebaiknya memberitahukan langkah-langkah dalam perlindungan dan antisipasi kepada nasabah dan Melakukan pemulihan yang mengacu pada UU27/2022 PP 71/2019

DAFTAR PUSTAKA**Jurnal**

- Ardhian, I. R. N. (2023). Dampak serangan siber dan kebocoran data pada perbankan syariah terhadap tingkat kepercayaan nasabah. *Maliki Interdisciplinary Journal*, 1(3), 351–359.
- Badruzaman, D. (2018). Prinsip-Prinsip Muamalah dan Implementasinya Dalam Hukum Perbankan Indonesia. *Jurnal Ekonomi Syariah Dan Bisnis*, 1(2), 109–116.
- Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data. *Padjadjaran Law Review*, 9(1).
- Gaib, D. N. (2019). Dinamika Hukum Perbankan Digital di Indonesia. *Lex Et Societatis*, 7(11).
- I GEDE WAHYU, Y. (2024). *TANGGUNG JAWAB HUKUM BANK TERHADAP KEBOCORAN DATA NASABAH AKIBAT TINDAKAN PERETASAN DALAM PERSPEKTIF HUKUM POSITIF DI INDONESIA*. Universitas Mataram.
- Irfansyah, K., & Qomaruddin, H. (2023). *KEBOCORAN DATA NASABAH PERBANKAN DALAM PERSPEKTIF HUKUM PIDANA (Analisis Kasus Kebocoran Data Nasabah Bank BSI)*. Sekolah Tinggi Ilmu Hukum IBLAM.
- MA'RIFA, H. S. F. (2023). *PENGARUH KEBOCORAN DATA (RANSOMWARE) DAN KUALITAS LAYANAN TERHADAP LOYALITAS NASABAH BANK SYARIAH INDONESIA DI PROVINSI JAWA TENGAH*. UNDIP: Fakultas Ekonomika & Bisnis.
- Marcelliana, V., Zahra, S. M., Adzani, N. N., Massaid, H. N., Badriyyah, N., Benita, R., Fitriani, C. N., & Bayhaqi, T. A. R. (2023). Penerapan Perlindungan Konsumen Terhadap Nasabah Pt. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah. *Depositi: Jurnal Publikasi Ilmu Hukum*, 1(2), 180–194.
- Mochtar, M. B. (2023). Kepastian Hukum Atas Kebocoran Data Pribadi Pengguna Aplikasi Online. *YUSTISIA MERDEKA: Jurnal Ilmiah Hukum*, 9(2), 1–12.
- Nurhasanah, N., Adam, P., & Listianingsih, D. M. (2017). *Hukum Perbankan Syariah: Konsep dan Regulasi*.
- Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. com). *Borneo Law Review*, 5(1), 46–68.
- Putri, D. F., Sari, W. R., & Nabbila, F. L. (2023). ANALISIS PERLINDUNGAN NASABAH BSI TERHADAP KEBOCORAN DATA DALAM MENGGUNAKAN DIGITAL BANKING. *Jurnal Ilmiah Ekonomi Dan Manajemen*, 1(4), 173–181.
- Rachmadi Usman, S. H. (2022). *Aspek hukum perbankan syariah di Indonesia*. Sinar Grafika.
- Rahmawati, I. N., Rahmadani, N., Heni, D. R., & Kevin, S. (2023). Pertanggung jawaban Pihak Bank terhadap Kebocoran Data Diri Nasabah. *Aufklarung: Jurnal Pendidikan, Sosial Dan Humaniora*, 3(2), 208–215.
- Raineven, S. V. C. (2023). *Perlindungan Hukum Bagi Konsumen yang Mengalami Kebocoran Data Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Di Indonesia*.

Sinaga, G. G., Jusuf, A. S., Kornelius, Y., & Tarina, D. D. Y. (2023). Analisis Peran Otoritas Jasa Keuangan Terhadap Perbankan Sebagai Upaya Perlindungan Data Pribadi Nasabah Bank (Studi Kasus Kebocoran Data Nasabah Bank Syariah Indonesia). *Jurnal Pendidikan Tambusai*, 7(3), 28374–28383.

Buku

Sunardi, D. (2021). *Hukum Perbankan dan Perbankan Syariah*. Penerbit A-Empat.

Usanti, T. P., & Shomad, A. (2017). *Hukum Perbankan*. Kencana.

Yusmad, M. A. (2018). *Aspek Hukum Perbankan Syariah dari Teori ke Praktik*. Deepublish.