Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 501-504

Analisis Hukum Dalam Kasus Serangan Siber Pada Bank Syariah Indonesia (BSI)

Faiz Raudhin Zulfikar[1], Airiique Bintang Merah Harley[2]
[12]Program Studi Hukum, Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta
Email: faizoktober@gmail.com, erikharli@gmail.com

Abstract
The case of the breach of Bank Syariah Indonesia (BSI) by the LockBit 3.0 hacker group that occurred on May 8, 2023 became one of the largest cybersecurity incidents in Indonesia. With the theft of personal data of more than 15 million customers, this incident had a significant impact on public trust and data security in the banking sector. This research uses a normative juridical method to analyze how regulations related to cyber attacks that occur against banks are regulated which include rights, obligations of both institutions and customers as well as administrative and criminal sanctions that can be given to protect customer interests. The results showed that the regulation related to cyber attacks in Indonesia has been regulated in the Law and the cause of the hacking case that occurred was because Bank Syariah Indonesia (BSI) did not pay sufficient attention to the digital security system used.

Article History
Received Okt 27, 2024
Revised Okt 29, 2024
Accepted 19 Nov 2024
Available online 24 Nov. 2024

Keywords :
LockBit, Cyber, BSI

Abstract
Kasus pembobolan Bank Syariah Indonesia (BSI) oleh kelompok hacker LockBit 3.0 yang terjadi pada 8 Mei 2023 menjadi salah satu insiden keamanan siber terbesar di Indonesia. Dengan pencurian data pribadi lebih dari 15 juta nasabah, insiden ini menimbulkan dampak signifikan terhadap kepercayaan publik dan keamanan data di sektor perbankan. Penelitian ini menggunakan metode yuridis normatif untuk menganalisis bagaimana peraturan terkait dengan adanya serangan cyber yang terjadi terhadap perbankan diatur yang mencakup hak, kewajiban baik lembaga maupun nasabah serta sanksi administratif dan pidana yang dapat diberikan untuk melindungi kepentingan nasabah. Hasil penelitian menunjukkan bahwa pengaturan terkait serangan cyber di Indonesia telah diatur dalam UU dan penyebab adanya kasus peretasan yang terjadi adalah karena Bank Syariah Indonesia (BSI) kurang memperhatikan sistem keamanan digital yang digunakan.

Keywords :
LockBit, Cyber, BSI.

https://doi.org/10.5281/zenodo.14216236

This is an open-access article under the **CC-BY-SA License.**

PENDAHULUAN

Perbankan adalah sebuah industri berfungsi sebagai lembaga keuangan yang utama dalam menerima simpanan giro, tabungan, dan deposito. Dengan demikian, perbankan memiliki beberapa tujuan strategis, antara lain mendukung pelaksanaan pembangunan nasional, meningkatkan pemerataan pembangunan, serta mendorong pertumbuhan ekonomi. [1]Selain itu, perbankan juga berperan penting dalam menjaga stabilitas nasional, yang pada akhirnya bertujuan untuk meningkatkan kesejahteraan masyarakat secara keseluruhan.[1] pada masa saat ini dimana dunia sudah mulai beralih dari teknologi tradisional menuju teknologi modern juga telah mengubah bagaimana sistem perbankan berjalan, salah satunya adalah dengan adanya transformasi digital pada sistem perbankan ditandai dengan lahirnya layanan bank online (*mobile banking)* Perkembangan pesat sektor fintech di Indonesia telah mengubah pola perilaku masyarakat dalam melakukan transaksi keuangan. Transaksi keuangan digital terus mengalami pertumbuhan yang signifikan, seiring dengan meningkatnya penggunaan platform e-commerce.

Kehadiran mobile banking di Indonesia telah mempermudah nasabah dalam menyelesaikan urusan perbankan hanya dalam hitungan menit, kapan saja dan di mana saja.[2] Perubahan digitalisasi telah diimplementasikan oleh berbagai institusi perbankan, termasuk PT Bank Syariah Indonesia Tbk (BSI). Pada tanggal 1 Februari 2021, BSI mencatatkansebuah sejarah baru sebagai hasil merger antara PT Bank BRI syariah Tbk, PT Bank Syariah Mandiri, dan PT Bank BNI Syariah. Merger ini disahkan

[1] Watung, R. W., & Ilat, V. (2016). Pengaruh Return On Asset (Roa), Net Profit Margin (Npm), Dan Earning Per Share (Eps) Terhadap Harga Saham Pada Perusahaan Perbankan Di Bursa Efek Indonesia Periode 2011-2015. Jurnal EMBA: Jurnal Riset Ekonomi, Manajemen, Bisnis dan Akuntansi, 4(2).
[2] Suharbi, M. A., & Margono, H. (2022). Kebutuhan transformasi bank digital Indonesia di era revolusi industri 4.0. Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan, 4(10), 4749-4759.

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 501-504

melalui Surat Keputusan Otoritas Jasa Keuangan (OJK) No. 04/KDK.03/2021. Dimana pada saat yang bersamaan Bank BSI juga mengeluarkan layanan perbankan digital bernama BSI Mobile sebagai bentuk transformasi digital guna memenuhi kebutuhan masyarakat pada era yang serba modern dengan perkembangan teknologi yang begitu pesat.

Dalam pelaksanaanya tentu tidak lepas dari adanya potensi risiko yang dapat terjadi, Risiko sendiri memiliki arti adanya potensi kerugian yang dapat timbul sebagai akibat dari terjadinya suatu peristiwa tertentu.[3] Keberadaan sistem digital di perbankan BSI membawa risiko terkait potensi ancaman kejahatan siber yang dapat membahayakan data pribadi nasabah. Di Indonesia, beberapa jenis kejahatan siber yang sering terjadi antara lain peretasan (hacking), cracking, penipuan kartu kredit (carding), skimming ATM, dan phishing. Frekuensi tinggi kasus ancaman siber saat ini dipengaruhi oleh berbagai faktor, termasuk meningkatnya akses penggunadi internet.[4]

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yang berarti fokusnya adalah pada analisis norma-norma hukum yang tertulis dalam peraturan perundang-undangan. Jenis penelitian ini dikategorikan sebagai penelitian hukum normatif, di mana norma hukum yang ditelaah bisa bersumber dari peraturan perundang-undangan. Secara lebih luas, penelitian normatif mengkaji norma dan asas hukum, baik yang tercantum dalam peraturan perundang-undangan maupun yang tidak. Sumber hukum primer diambil dari Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sementara sumber hukum sekunder diambil melalui kajian terhadap literatur hukum yang berkaitan dengan perbankan, jurnal, dan internet. Metode pengumpulan data yang digunakan dalam penelitian ini adalah studi kepustakaan. Artinya, informasi dan data diperoleh dengan cara membaca dan menganalisis berbagai sumber tertulis, seperti buku, jurnal, dan website.

HASIL DAN PEMBAHASAN

Kasus ini bermula dari adanya kesalahan sistem yang mengakibatkan baik nasabah maupun kantor cabang tidak dapat melakukan transaksi melalui ATM maupun BSI Mobile. pada tanggal 8 Mei 2023, lewat akun instagram Pihak BSI mengumumkan adanya kendala dan gangguan pada sistem perbankan BSI karena sedang adanya pemeliharaan sistem berupa perbaikan dan migrasi sistem namun gangguan ini terus terjadi selama berhari hari.

Pada tanggal 10 Mei 2023, Menteri BUMN Erick Thohir mengajukan pertanyaan mengenai potensi serangan siber yang mungkin terjadi. Satu hari setelahnya, pihak Bank Syariah Indonesia (BSI) mengadakan konferensi pers, di mana mereka mengonfirmasi adanya serangan siber yang mengakibatkan gangguan pada layanan perbankan mereka. Meskipun layanan BSI berhasil pulih pada hari yang sama, pihak bank belum memberikan penjelasan mengenai jenis serangan siber yang dialami, karena masih memerlukan proses audit dan forensik digital untuk memperoleh bukti yang lebih jelas.

Pada 12 Mei 2023, Beredar sebuah klaim mengenai adanya gangguan pada layanan BSI terjadi karena adanya aktivitas dari peretas. Kelompok peretas yang dikenal dengan nama LockBit mengklaim bahwa mereka telah berhasil menyerang sistem BSI menggunakan ransomware LockBit 3.0. Informasi mengenai klaim ini pertama kali disampaikan kepada publik melalui akun Twitter @darktracer_int pada 13 Mei 2023. Menurut data yang diklaim, Data sensitif baik milik nasabah maupun perusahaan yang telah dicuri berukuran 1.5TB (terabyte) dari 9 pusat data (database) yang berisikan 15 juta data nasabah dan karyawan, data sensitif yang dimaksud diantaranya

1. Nomor Telepon,
2. Alamat Lengkap,
3. Nama Lengkap,
4. Rincian dokumen,

[3] Sudarmanto, E., Astuti, A., Kato, I., Basmar, E., Simarmata, H. M. P., Yuniningsih, Y., ... & Siagian, V. (2021). Manajemen Risiko Perbankan.
[4] Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT), 1(2), 85-92.

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 501-504

5. Informasi Saldo bank, nomor kartu riwayat transaksi, serta dokumen-dokumenfinansial,
6. Surat hukum, dan perjanjian kerahasiaan (NDA).
7. Data kata sandi untuk semua layanan internal dan eksternal yang digunakan olehbank.

Peretas juga mengancam akan membocorkan data nasabah dengan memberikan waktu 72Jam untuk menghubunginya sebagai jalan penyelesaian masalah namun tidak ada respon yang diberikan sehingga pada tanggal 16 Mei pada pukul 7 pagi peretas membocorkan data yang telah dicuri di situs dark web karena tidak mencapai kesepakatan yang tawarkan. Peretas meminta BSImembayar tebusan sebesar 20 juta Dolar AS (Rp 296.4 Miliar) kemudian ditawar dengan nominal 100 Ribu dan 10 Juta dollar AS namun keduanya ditolak oleh peretas

Analisis hukum

Dalam kasus ini terdapat beberapa pelanggaran yang dilakukan oleh bank BSI dan dapat dibedakan dengan dilihat bedasarkan Undang Undang yang relevan

a. UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Berdasarkan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi pada pasal 57 ayat 1 menjelaskan terkait dengan pelanggaran yang dapat dikenakan sanksi, dan dalam kasus ini pelanggaran pada pasal 20. Pada pasal 20 ayat 2 dijelaskan beberapa ketentuan dasar yang menjadi dasar dalam melakukan pemrosesan data pribadi dan dalam kasus ini pihak bank BSI tidak berhasil memenuhi hal tersebut dengan bocornya data pribadi nasabah yang merupakan hak subjek data pribadi, hal ini diperjelas dengan pasal 4 ayat 2 huruf yang menegaskan bahwa data keuangan pribadi merupakan data spesifik yang melekat kepada subjek data dalam hal ini adalah nasabah. Dampak dari tidak dipenuhinya kewajiban ini dijelaskan pada pasal 57 ayat 1, 2 dan 3 yang masing masing menjelaskan tentang pelanggaran pasal, sanksi administratif dan denda administratif yang dapat dijatuhkan

b. UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Berdasarkan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pada pasal 30 ayat 1, 2, dan 3 menjelaskan terkait dengan adanya kesenjangan seseorang dan tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik untuk mendapatkan informasi. Dalam hal ini peretas berhasil masuk kedalam sistem elektronik bank BSI dengan cara menyusupkan malware LockBit 3.0. Dan ini berhasil melampaui sistem keamanan bank BSI dengan cara menerobos dan menjebol sistem keamanan yang ada. Menurut pasal 46 ayat 1,2 dan 3. Ketentuan pidana yang dapat diberikan adalah penjara paling lama 6 sampai 8 tahun dan denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah) sampai Rp800.000.000,00 (delapan ratus juta rupiah).[5]

Pada pasal 32 ayat 1, 2 dan 3 menjelaskan terkait dengan adanya pengubahan atau perpindahan data secara melawan hukum bari dari/oleh orang yang tidak berhak melakukan perpindahan. Dalam kasus ini sebanyak 15 juta datanasabah berhasil dipindahkan dari 9 pusat data dan kemudian digunakan tidak sebagaimana mestinya dalam kasus ini dijual kepada publik lewat situs dark web seharga 20 juta Dolar AS. Menurut pasal 48 ayat 1,2 dan 3. Ketentuan pidana yang dapat diberikan adalah penjara paling lama 8 sampai 10 tahun dan denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah) sampai Rp5.000.000.000,00 (lima miliar rupiah).

Pada pasal 33 menjelaskan terkait dengan adanya gangguan dalam sistem elektronik yang menyebabkan tidak dapat bekerja sebagaimana mestinya. Dalam kasus ini adanya serangan yang terjadi menyebabkan layanan BSI mulai dari perbankan sampai bank online terganggu selama beberapa hari. menurut pasal 49 ketentuan pidana yang dapat diberikan adalah penjara paling lama 10 tahun dan denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah)

SIMPULAN

Kasus pembobolan Bank Syariah Indonesia (BSI) oleh kelompok hacker LockBit 3.0 menyoroti tantangan serius yang dihadapi sektor perbankan di era digital, khususnya terkait keamanan siber. Pencurian data pribadi lebih dari 15 juta nasabah, termasuk informasi sensitif seperti nomor telepon dan saldo rekening, mengakibatkan kerugian tidak hanya bagi bank, tetapi juga berpotensi menimbulkan risiko signifikan bagi nasabah yang terkena dampak. Dari sudut pandang hukum, insiden

[5] UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik digunakan karena UU Nomor 19 Tahun 2016 tidak memberikan perubahan apapun pada pasal yang dimaksud dan undang undang terbaru dibuat setelah adanya kasus sehingga tidak relevan digunakan

November 2024. Vol. 2, No. 4
e-ISSN: 3032-6591
pp 501-504

ini melanggar Undang-Undang terutama terkait dengan Perlindungan Data Pribadi (UU PDP) dan Informasi dan Transaksi Elektronik (UU ITE). Jika terbukti gagal dalam melindungi data nasabah sesuai ketentuan yang berlaku, BSI berpotensi menghadapisanksi administratif dan pidana. Kasus ini juga menunjukan betapa pentingnya peningkatan sistem keamanan siber di lembaga keuangan. Mengingat ancaman kejahatan siber yang terus berkembang, bank perlu berinvestasi dalam teknologi keamanan yang lebih inovatif dan memberikan pelatihan kepada karyawan untuk mampu mengenali dan menangani potensi ancaman di masa yang akan mendatang.

REFERENSI

Watung, R. W., & Ilat, V. (2016). Pengaruh Return On Asset (Roa), Net Profit Margin (Npm), Dan Earning Per Share (Eps) Terhadap Harga Saham Pada Perusahaan Perbankan Di Bursa Efek Indonesia Periode 2011-2015. Jurnal EMBA: Jurnal Riset Ekonomi, Manajemen, Bisnis dan Akuntansi, 4(2).

Suharbi, M. A., & Margono, H. (2022). Kebutuhan transformasi bank digital Indonesia diera revolusi industri 4.0. Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan, 4(10), 4749-4759.

Sudarmanto, E., Astuti, A., Kato, I., Basmar, E., Simarmata, H. M. P., Yuniningsih, Y., ...& Siagian, V. (2021). Manajemen Risiko Perbankan.

Undang-undang (UU) Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Undang-undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik