**Al-Zayn: Jurnal Ilmu Sosial & Hukum** e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 1, 2026
DOI: https://doi.org/10.61104/alz.v4i1.3146

# *Strict liability vs fault based* : Perbandingan Indonesia dengan Jepang Terhadap Kebocoran Data

**Angelica Suciara[1], Bryan Idias[2], Nathasya Jhonray Siregar[3], Tasya Amira Frananda Siregar[4] , Tri Widyasto Prabowo[5]**
Fakultas Hukum, Universitas Pelita Harapan, Indonesia
*Email Korespondensi: 01051230167@student.uph.edu, 01051230200@student.uph.edu, 01051230196@student.uph.edu, 01051230179@student.uph.edu, 01051230172@student.uph.edu*

*Article received: 01 November 2025, Review process: 11 November 2025*
*Article Accepted: 25 Desmber 2025, Article published: 01 Januari 2026*

***ABSTRACT***
*This study examines the application of the principle of Unlawful Act (Perbuatan Melawan Hukum / PMH) in banking data breach cases through a comparative analysis between Indonesia and Japan. The discussion focuses on the proof of fault by banks, the burden of proof on customers, and the relevance of applying strict liability compared to fault-based liability within the framework of data protection in the banking sector. The 2024 data breach incident involving Bank Syariah Indonesia (BSI) demonstrates the weakness of legal protection for customers due to the fault-oriented nature of Indonesia's civil liability system, as stipulated in Article 1865 of the Indonesian Civil Code, which places the burden of proof on the claimant. In contrast, the cyberattack case against Mitsubishi UFJ Financial Group (MUFG) in Japan illustrates a more objective approach to liability, where financial institutions remain responsible for consumer losses even when negligence is not fully established. Using a juridical-comparative method, this study finds that the adoption of strict liability is more appropriate in modern banking data protection, as it ensures a fairer balance between institutional accountability and the substantive rights of customers. The findings recommend a reformulation of Indonesia's legal framework on banking liability to strengthen consumer protection against data breaches.*
***Keywords:*** *Unlawful Act (PMH), banking data breach, strict liability, fault-based liability, consumer protection.*

**ABSTRAK**
*Penelitian ini membahas penerapan prinsip Perbuatan Melawan Hukum (PMH) dalam kasus kebocoran data perbankan dengan melakukan studi komparatif antara Indonesia dan Jepang. Fokus kajian diarahkan pada pembuktian unsur kesalahan bank, beban pembuktian nasabah, serta relevansi penerapan prinsip strict liability dibandingkan fault-based liability dalam konteks perlindungan data nasabah. Kasus kebocoran data Bank Syariah Indonesia (BSI) tahun 2024 menunjukkan lemahnya perlindungan hukum terhadap nasabah akibat sistem pembuktian yang masih berorientasi pada kesalahan, sebagaimana diatur dalam Pasal 1865 KUH Perdata, yang membebankan kewajiban pembuktian kepada pihak yang mendalilkan haknya. Sebaliknya, kasus serangan siber terhadap Mitsubishi UFJ Financial Group (MUFG) di Jepang memperlihatkan penerapan mekanisme pertanggungjawaban yang lebih objektif, di mana lembaga keuangan tetap memikul tanggung jawab atas kerugian konsumen meskipun unsur kelalaian belum terbukti secara penuh. Melalui pendekatan yuridis-komparatif, penelitian ini menemukan bahwa penerapan strict liability lebih sesuai*

 

*untuk konteks perlindungan data perbankan modern, karena memberikan keseimbangan antara tanggung jawab lembaga keuangan dan hak nasabah dalam memperoleh keadilan substantif. Temuan ini merekomendasikan perlunya reformulasi sistem pertanggungjawaban hukum perbankan di Indonesia untuk memperkuat perlindungan terhadap kebocoran data pribadi.*
***Kata Kunci**: Perbuatan Melawan Hukum, kebocoran data perbankan, strict liability, fault-based liability, perlindungan konsumen*

## PENDAHULUAN

Perkembangan teknologi informasi dalam sektor perbankan telah membawa perubahan besar terhadap sistem pelayanan keuangan modern. Digitalisasi perbankan memungkinkan kemudahan akses, efisiensi transaksi, dan personalisasi layanan bagi nasabah. Namun, kemajuan ini juga diiringi dengan meningkatnya risiko keamanan data pribadi. Dalam konteks hukum, kebocoran data perbankan menimbulkan persoalan penting mengenai tanggung jawab hukum bank terhadap kerugian nasabah, terutama ketika data nasabah disalahgunakan atau dipublikasikan tanpa izin.

Kasus kebocoran data dalam sektor keuangan Indonesia menegaskan lemahnya perlindungan keamanan digital serta mekanisme pertanggungjawaban hukum lembaga keuangan. Salah satu contoh paling menonjol adalah insiden Bank Syariah Indonesia (BSI) pada Mei 2023, ketika kelompok *ransomware LockBit* 3.0 mengklaim berhasil mencuri sekitar 1,5 *terabyte* data berisi informasi lebih dari 15 juta nasabah dan karyawan (Indonesia *Business Post*, 2023). Kebocoran tersebut berdampak pada kepercayaan publik terhadap keamanan sistem perbankan nasional, serta memunculkan pertanyaan mengenai tanggung jawab hukum bank terhadap nasabah.

Situasi ini menunjukkan adanya kekosongan dalam mekanisme pembuktian kesalahan dan beban tanggung jawab antara bank dan nasabah. Di satu sisi, nasabah seringkali berada pada posisi lemah karena keterbatasan akses terhadap bukti sistem internal bank. Di sisi lain, bank cenderung berargumen bahwa serangan siber merupakan peristiwa *force majeure* yang sulit dihindari. Hal ini menimbulkan perdebatan mengenai dasar tanggung jawab hukum, apakah didasarkan pada kesalahan (*fault-based liability*) atau tanggung jawab mutlak (*strict liability*) yang tidak bergantung pada pembuktian kesalahan.

Untuk memahami dasar pertanggungjawaban hukum dalam pelanggaran data pribadi, perlu terlebih dahulu melihat konsep tanggung jawab perdata sebagai fondasi dalam hukum internasional maupun domestik. Dalam doktrin hukum, *Fault-based liability arises when a party is responsible for failure or error Meanwhile, strict liability occurs when a party is responsible for its actions that cause losses, regardless of whether the party was at fault or negligent* (Atmadja et al., 2025) yang jika diartikan, *Fault-based liability* atau tanggung jawab berdasarkan kesalahan merupakan prinsip hukum yang menempatkan seseorang sebagai pihak yang bertanggung jawab hanya apabila terbukti melakukan kesalahan, baik karena kelalaian (*negligence*) maupun perbuatan yang disengaja (*intentional fault*). Dalam sistem ini, beban pembuktian berada pada pihak yang dirugikan untuk menunjukkan bahwa

 

kerugian yang terjadi disebabkan oleh tindakan salah dari pihak yang dituntut. Dengan demikian, jika tidak terdapat kesalahan, maka tidak ada tanggung jawab hukum yang dapat dibebankan.

Sebaliknya, *strict liability* atau tanggung jawab mutlak adalah prinsip yang menetapkan bahwa seseorang tetap bertanggung jawab atas kerugian yang ditimbulkan akibat tindakannya, meskipun ia tidak terbukti lalai atau bersalah. Dalam sistem ini, cukup dibuktikan adanya hubungan sebab-akibat antara tindakan pelaku dan kerugian yang terjadi untuk menimbulkan tanggung jawab hukum. Konsep *strict liability* banyak diterapkan pada bidang-bidang dengan risiko tinggi, seperti pengelolaan data digital, lingkungan, dan industri teknologi, karena kerugian dapat timbul meskipun pihak pelaku telah berhati-hati.

Di Jepang, negara yang memiliki sistem perlindungan data pribadi relatif lebih matang melalui *Act on the Protection of Personal Information* (APPI). Pada tahun fiskal 2024, Jepang mencatat 19.056 kasus kebocoran data pribadi, angka tertinggi sepanjang sejarah dan menunjukkan peningkatan sekitar 57% dibandingkan tahun sebelumnya. Lonjakan ini menggambarkan semakin seriusnya risiko keamanan siber serta kebutuhan akan mekanisme perlindungan data yang lebih kuat (*The Japan Times*, 2024). Salah satu kasus yang cukup menonjol adalah pelanggaran yang melibatkan *Mitsubishi UFJ Financial Group* (MUFG), ketika otoritas pengawas keuangan Jepang merekomendasikan tindakan terhadap unit perbankan dan sekuritasnya akibat praktik pembagian data klien tanpa izin. Kasus ini menyoroti lemahnya kepatuhan internal serta risiko penyalahgunaan data dalam sektor keuangan (Reuters, 2024). Kasus ini memperlihatkan bagaimana lembaga keuangan di Jepang dapat dimintai pertanggungjawaban hukum bahkan atas pelanggaran prinsip *consent* (persetujuan).

Perbandingan antara Indonesia dan Jepang menjadi menarik karena kedua negara menghadapi risiko yang sama, tetapi memiliki sistem hukum dan pendekatan tanggung jawab yang berbeda. Indonesia masih menitikberatkan tanggung jawab berdasarkan kesalahan (*fault-based*), sebagaimana diatur dalam Pasal 1365 KUHPerdata, sedangkan Jepang mulai menunjukkan kecenderungan ke arah penerapan prinsip tanggung jawab yang lebih ketat dalam konteks perlindungan data pribadi.

Dengan demikian, penelitian ini penting untuk mengkaji bagaimana penerapan Perbuatan Melawan Hukum (PMH) dalam kasus pelanggaran keamanan data perbankan, dengan fokus pada pembuktian unsur kesalahan bank, beban pembuktian nasabah, serta kemungkinan penerapan *strict liability* sebagai alternatif dalam memperkuat perlindungan hukum terhadap nasabah. Studi komparatif antara Indonesia dan Jepang diharapkan dapat memberikan pemahaman yang lebih komprehensif mengenai arah perkembangan tanggung jawab hukum lembaga keuangan di era digital.

## METODE

Penelitian ini merupakan penelitian yuridis normatif yang dikombinasikan dengan pendekatan komparatif (comparative approach). Pendekatan yuridis normatif digunakan untuk menganalisis peraturan perundang-undangan, doktrin

hukum, serta prinsip-prinsip Perbuatan Melawan Hukum (PMH) yang berkaitan dengan tanggung jawab atas kebocoran data perbankan di Indonesia dan Jepang, sedangkan pendekatan komparatif digunakan untuk menelaah perbedaan penerapan tanggung jawab hukum, pembuktian kesalahan, serta mekanisme perlindungan nasabah di kedua negara sehingga penelitian ini tidak hanya bersifat deskriptif-analitis, tetapi juga berupaya mengidentifikasi model hukum ideal yang dapat diterapkan di Indonesia. Data penelitian bersumber dari bahan hukum primer yang meliputi KUH Perdata Pasal 1365, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 21 Tahun 2011 tentang OJK, Act on the Protection of Personal Information (APPI) Jepang, serta regulasi OJK dan Kominfo terkait keamanan siber perbankan; bahan hukum sekunder berupa literatur dan jurnal hukum mengenai PMH, data protection, strict liability, laporan resmi serta publikasi lembaga seperti PPC Japan, Kominfo, dan OJK; serta bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, dan sumber daring relevan untuk memperjelas konsep dan istilah hukum yang digunakan.

## HASIL DAN PEMBAHASAN

### *Penerapan Unsur PMH dalam Pelanggaran Keamanan Data di Indonesia dan Jepang*

Dalam sistem hukum Indonesia, tanggung jawab perdata atas kebocoran data diatur secara umum melalui Pasal 1365 KUHPerdata, yang menegaskan bahwa setiap perbuatan melanggar hukum yang menimbulkan kerugian pada orang lain mewajibkan pelaku untuk mengganti kerugian, empat unsur utama yang harus dibuktikan untuk menyatakan suatu pihak melakukan PMH adalah ketika terdapat perbuatan melawan hukum, terdapat kesalahan, terdapat kerugian, dan juga terdapat hubungan kausal antara perbuatan dan kerugian

### *Unsur Kesalahan*

Unsur kesalahan yang dilakukan dapat berbentuk kesengajaan ataupun kelalaian. Dalam konteks kebocoran data, unsur kesalahan umumnya berbentuk kelalaian bank dalam menjalankan kewajiban pengamanan data nasabah. Seperti halnya, bank tidak memperbarui sistem keamanan atau enkripsi sesuai standar terbaru, lalai melakukan audit keamanan siber secara berkala, tidak segera menanggapi peringatan kebocoran (data breach alert), membiarkan akses internal tanpa kontrol otorisasi ketat.

Pada Mei 2023, BSI mengalami kebocoran data besar-besaran akibat serangan ransomware LockBit 3.0, yang menyebabkan gangguan layanan dan dugaan kebocoran data nasabah. Data yang bocor dilaporkan meliputi informasi pribadi seperti nomor KTP, rekening, dan data transaksi terhadap kejadian tersebut, terdapat indikasi kelalaian pada aspek berikut:

1. Kegagalan dalam menerapkan sistem keamanan sistem elektronik yang memadai sebagaimana diamanatkan oleh Pasal 24 ayat (3) UU No. 71 Tahun 2019

 

2. Keterlambatan dalam pelaporan dan transparansi kepada nasabah. Menurut Permenkominfo 20/2016 tentang Perlindungan Data Pribadi, pengendali data wajib memberitahukan kebocoran data "secepatnya" kepada pemilik data.
3. Tidak adanya audit keamanan independen yang dapat membuktikan upaya pencegahan yang cukup.

Dengan demikian, unsur kesalahan dapat dikategorikan sebagai kelalaian (negligence) karena bank lalai dalam menerapkan prinsip kehati-hatian (duty of care) terhadap data pribadi nasabahnya.

***Unsur Perbuatan Melawan Hukum***

Pada 2024, otoritas keuangan Jepang (Financial Services Agency / FSA) menjatuhkan tindakan administratif kepada Mitsubishi UFJ Financial Group dan unit sekuritas afiliasinya karena membagikan data nasabah secara tidak sah tanpa persetujuan nasabah sebanyak 26 kali antara 2020–2023. Kasus ini diungkap oleh Securities and Exchange Surveillance Commission (SESC) dan melanggar prinsip firewall yang diatur dalam sistem regulasi Jepang — yakni pemisahan data antara bank dan sekuritas untuk menjaga kerahasiaan nasabah. Sebagai respons atas pelanggaran tersebut, Financial Services Agency (FSA) Jepang memerintahkan MUFG untuk melakukan perbaikan menyeluruh terhadap sistem pengendalian internal serta memperkuat mekanisme kepatuhan terkait perlindungan data pribadi. Langkah ini menunjukkan ketegasan regulator dalam memastikan standar keamanan data yang lebih tinggi di sektor keuangan (Investing.com, 2024).

Berdasarkan, Act on the Protection of Personal Information (APPI) Jepang, lembaga keuangan wajib memastikan perlindungan, akurasi, dan integritas data pribadi dengan langkah yang "reasonably necessary and appropriate." Kegagalan MUFG dalam mencegah pembagian data tanpa persetujuan nasabah dinilai sebagai bentuk kelalaian institusional yang bersumber dari lemahnya tata kelola dan pengawasan internal, bukan akibat serangan eksternal. Pelanggaran ini bertentangan dengan ketentuan Act on the Protection of Personal Information (APPI), khususnya Pasal 23–24 hasil amendemen 2020, yang mewajibkan persetujuan eksplisit serta penerapan kontrol internal yang memadai dalam pemrosesan data pribadi.

Namun, sistem hukum Jepang menempatkan beban pembuktian pada lembaga keuangan, bukan nasabah, untuk menunjukkan bahwa prosedur kepatuhan dan pengendalian internal telah diterapkan dengan benar. Dengan demikian, unsur kesalahan dalam konteks Jepang terbukti, tetapi mekanisme akuntabilitasnya bersifat kooperatif dan korektif, bukan represif seperti gugatan PMH di Indonesia.

Dalam konteks kebocoran data perbankan tahun 2023, BSI dapat dianggap melakukan perbuatan melawan hukum karena:

1. Melanggar kewajiban hukum yang diatur dalam Pasal 24 ayat (2) UU nomor 71 tahun 2019, yang mewajibkan Penyelenggara Sistem Elektronik menjaga keamanan sistemnya.

 

2. Melanggar hak subjektif nasabah, yakni hak atas privasi dan perlindungan data pribadi, sebagaimana dijamin dalam Pasal 2 huruf a Permenkominfo No. 20 Tahun 2016.
3. Bertentangan dengan asas kepatutan dan kehati-hatian (due care) yang menjadi standar etis dalam perbankan dan pengelolaan data.

Dengan demikian, tindakan BSI yang gagal melindungi data nasabah memenuhi unsur melawan hukum, karena bertentangan dengan ketentuan peraturan perundang-undangan serta prinsip kepatutan dan tanggung jawab sosial perbankan.

Kasus pelanggaran yang dilakukan MUFG antara tahun 2020–2023 menunjukkan bahwa bank dan unit sekuritas afiliasinya telah membagikan data klien secara tidak sah tanpa persetujuan nasabah sebanyak 26 kali. Tindakan ini melanggar:

1. Ketentuan eksplisit dalam Pasal 23 APPI mengenai larangan berbagi data tanpa persetujuan.
2. Prinsip firewall regulation yang diterapkan oleh Financial Services Agency (FSA) untuk menjaga pemisahan data antar-unit bisnis.

Sanksi administratif kemudian dijatuhkan oleh FSA, yang memerintahkan MUFG untuk memperkuat kepatuhan internal dan memperbaiki sistem pengendalian data. Oleh karena itu, dalam konteks hukum Jepang, perbuatan MUFG termasuk kategori "melawan hukum" secara administratif, bukan perdata individual. Fokusnya bukan pada fault-based liability seperti di Indonesia, melainkan pada pelanggaran kewajiban kepatuhan lembaga (institutional compliance breach).

Hal ini menunjukkan bahwa Indonesia masih berorientasi pada pemidanaan atau gugatan perdata individual yang menuntut pembuktian kesalahan dan pelanggaran oleh pihak penggugat sementara Jepang menekankan akuntabilitas kelembagaan, di mana pelanggaran terhadap perlindungan data dianggap sebagai kegagalan sistem kepatuhan, bukan sekadar kesalahan individu.

***Unsur Kerugian***

Kebocoran data nasabah BSI pada Mei 2023 yang diduga dilakukan oleh kelompok ransomware LockBit 3.0 menimbulkan berbagai bentuk kerugian, baik materiil maupun immateriil:

1. Kerugian materiil: potensi kehilangan dana akibat akses ilegal terhadap rekening, potensi penipuan lanjutan (phishing, social engineering), serta gangguan terhadap transaksi bisnis nasabah.
2. Kerugian immateriil: ketidaknyamanan, kehilangan rasa aman, dan menurunnya kepercayaan publik terhadap sistem perbankan syariah nasional.
3. Beberapa laporan menyebutkan bahwa data seperti Nomor Induk Kependudukan (NIK), alamat, dan informasi rekening telah diperjualbelikan

di forum gelap, yang memperkuat adanya dampak langsung pada privasi nasabah.

Sama halnya dengan MUFG di Jepang yang mengalami insiden kebocoran data yang melibatkan kredensial pegawai dan akses ke sistem internal. Dampak kerugian yang dicatat oleh otoritas keuangan Jepang meliputi:

1. Kerugian materiil: potensi gangguan operasional dan biaya tinggi untuk pemulihan sistem serta kompensasi keamanan tambahan bagi nasabah.
2. Kerugian immateriil: kerusakan reputasi perusahaan dan kehilangan kepercayaan publik, yang diukur secara konkret melalui penurunan indeks kepercayaan pelanggan dan evaluasi reputasi oleh Financial Services Agency (FSA).
3. Di bawah hukum Jepang, terutama Act on the Protection of Personal Information (APPI), perusahaan yang lalai menjaga data pribadi wajib memberikan kompensasi langsung kepada pihak terdampak tanpa harus membuktikan kesalahan individu (pendekatan semi-strict liability).

***Unsur Sebab-Akibat***

Dalam kasus kebocoran data BSI, unsur kausalitas menjadi titik krusial karena sulit membuktikan hubungan langsung antara tindakan kelalaian bank dan kerugian yang dialami nasabah. Faktor-faktor yang memperumit unsur ini meliputi:

1. Sumber serangan eksternal: BSI mengklaim kebocoran terjadi akibat serangan siber dari pihak ketiga (ransomware LockBit 3.0), bukan karena kelalaian internal.
2. Kesulitan pelacakan digital evidence: nasabah sulit membuktikan bahwa data pribadinya bocor akibat kelalaian sistem keamanan BSI, bukan karena faktor eksternal atau kebocoran dari pihak lain.
3. Regulasi yang belum mengatur mekanisme pembuktian siber secara rinci: meski UU Perlindungan Data Pribadi No. 27 Tahun 2022 telah berlaku, mekanisme forensic audit dan tanggung jawab pembuktian belum sepenuhnya operasional di tingkat litigasi.

Dalam kasus MUFG (2024), unsur kausalitas lebih mudah ditegakkan karena Jepang menganut pendekatan hukum yang lebih presumeratif terhadap tanggung jawab lembaga keuangan.

1. Setelah insiden kebocoran data internal MUFG, Financial Services Agency (FSA) segera menyimpulkan adanya direct causal link antara kelemahan sistem keamanan internal MUFG dan potensi penyebaran data.
2. Di bawah Act on the Protection of Personal Information (APPI), jika terjadi pelanggaran keamanan, perusahaan dianggap bertanggung jawab langsung, kecuali dapat membuktikan bahwa insiden terjadi tanpa kelalaian atau kelengahan sistem internal.
3. Pendekatan ini disebut reversed burden of proof, di mana tanggung jawab pembuktian berpindah dari korban ke pihak pelaku usaha (bank).

 

4. MUFG diwajibkan melaporkan hasil audit internal, langkah remediasi, serta menyediakan kompensasi bagi nasabah terdampak tanpa memerlukan pembuktian kausalitas yang kompleks di pengadilan.

Secara keseluruhan, penerapan unsur Perbuatan Melawan Hukum (PMH) dalam kasus kebocoran data perbankan menunjukkan perbedaan mendasar antara Indonesia dan Jepang. Di Indonesia, seperti pada kasus Bank Syariah Indonesia (BSI), sistem hukum masih berorientasi pada fault-based liability, di mana nasabah sebagai penggugat wajib membuktikan unsur kesalahan, kerugian, dan hubungan kausalitas secara nyata. Hal ini menyulitkan nasabah karena keterbatasan akses bukti dan mekanisme forensik digital. Sebaliknya, di Jepang melalui kasus Mitsubishi UFJ Financial Group (MUFG), diterapkan prinsip semi-strict liability di bawah Act on the Protection of Personal Information (APPI) yang menempatkan tanggung jawab keamanan data pada lembaga keuangan. Akibatnya, beban pembuktian berpindah kepada bank, dan kerugian nasabah diakui secara lebih cepat melalui mekanisme audit dan kompensasi langsung. Dengan demikian, sistem Jepang menunjukkan pendekatan yang lebih protektif terhadap konsumen dan dapat menjadi model reformasi bagi sistem pembuktian dan tanggung jawab dataperbankandiIndonesia.

***Tanggung Jawab Hukum Bank dan Beban Pembuktian Nasabah di Indonesia dan Jepang***

Di Indonesia, prinsip pembuktian diatur dalam Pasal 1865 Kitab Undang-Undang Hukum Perdata (KUH Perdata), yang menegaskan bahwa "barang siapa yang mendalilkan suatu hak, maka ia wajib membuktikan dalilnya sendiri." Dalam konteks kebocoran data, hal ini berarti nasabah yang merasa dirugikan harus membuktikan bahwa kerugian yang dialaminya benar-benar disebabkan oleh kelalaian pihak bank. Prinsip ini membuat posisi nasabah menjadi lemah, karena bukti-bukti teknis seperti log sistem keamanan dan audit internal sepenuhnya berada dalam kendali pihak bank. Sebaliknya, di Jepang, sistem hukum melalui Act on the Protection of Personal Information (APPI) menerapkan prinsip semi-strict liability. Dalam kasus kebocoran data, lembaga keuangan otomatis dianggap bertanggung jawab, kecuali dapat membuktikan bahwa mereka telah melakukan semua langkah keamanan yang wajar sesuai standar nasional. Dengan demikian, beban pembuktian berpindah ke pihak bank, bukan nasabah. Prinsip ini melindungi konsumen secara lebih efektif dan memastikan akuntabilitas lembaga keuangan tetap terjaga.

Kasus Bank Syariah Indonesia (BSI) tahun 2024 menunjukkan masih lemahnya penerapan perlindungan data di sektor perbankan nasional. Kebocoran data lebih dari 15 juta nasabah mencakup informasi pribadi, nomor rekening, dan riwayat transaksi. Pemerintah melalui Kementerian Komunikasi dan Informatika (Kominfo) serta Otoritas Jasa Keuangan (OJK) kemudian melakukan langkah-langkah administratif, denga melakukan audit keamanan digital (digital forensic audit), memerintahkan penerapan Standar Keamanan Informasi ISO 27001, juga mewajibkan pelaporan insiden kepada Kominfo sebagaimana diatur dalam Pasal

 

46 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Namun, tidak ada mekanisme kompensasi langsung kepada nasabah, dan tanggung jawab bank masih bersifat fault-based, yaitu bergantung pada pembuktian adanya kesalahan pihak bank di pengadilan.

Sementara itu, dalam kasus Mitsubishi UFJ Financial Group (MUFG) Jepang tahun 2024, otoritas keuangan Financial Services Agency (FSA) bergerak cepat begitu laporan kebocoran muncul. Berdasarkan ketentuan APPI, MUFG diwajibkan untuk melakukan laporan resmi kepada FSA dan publik, melakukan audit internal dan evaluasi sistem keamanan, menyediakan kompensasi dan layanan pemulihan identitas bagi pihak terdampak. Pendekatan ini menunjukkan bahwa Jepang menempatkan tanggung jawab hukum yang bersifat preventif, bukan reaktif. Fokusnya adalah memulihkan kepercayaan publik dan memastikan perusahaan mengambil tindakan korektif segera.

***Penerapan prinsip strict liability jika diterapkan di Indonesia dalam konteks perlindungan data perbankan***

Sistem hukum Indonesia saat ini masih menganut prinsip fault-based liability dalam pertanggungjawaban perdata, sebagaimana tercermin dalam Pasal 1365 KUH Perdata, yang menegaskan bahwa tanggung jawab hanya timbul apabila dapat dibuktikan adanya unsur kesalahan (fault). Dalam konteks perlindungan data perbankan, sistem ini menimbulkan kesulitan praktis karena pihak nasabah yang dirugikan akibat kebocoran data sering kali tidak memiliki kemampuan teknis dan akses bukti untuk menunjukkan adanya kelalaian di pihak bank. Hal ini menyebabkan kesenjangan keadilan, karena nasabah tidak berada pada posisi yang setara dalam proses pembuktian terhadap lembaga keuangan yang memiliki sumber daya dan kendali penuh atas data.

Prinsip strict liability (tanggung jawab mutlak) menempatkan tanggung jawab pada pelaku usaha, dalam hal ini pihak bank, tanpa perlu dibuktikan adanya unsur kesalahan. Penerapan prinsip ini dinilai lebih relevan dalam perkara kebocoran data karena bank memiliki kendali eksklusif atas sistem dan infrastruktur keamanan data, sehingga secara logis mereka adalah pihak yang paling mampu mencegah dan mengendalikan risiko kebocoran, disisi lain nasabah berada dalam posisi lemah, baik secara teknis maupun hukum, untuk membuktikan unsur kesalahan, juga mendukung aspek sosial dan ekonomi, yakni menjaga kepercayaan publik terhadap sistem perbankan, menuntut adanya mekanisme tanggung jawab yang cepat dan efektif tanpa proses pembuktian yang rumit. Dalam sistem strict liability, tanggung jawab bank akan muncul secara otomatis ketika terjadi pelanggaran keamanan data, kecuali dapat dibuktikan bahwa insiden terjadi karena keadaan memaksa (force majeure) atau sepenuhnya akibat tindakan pihak ketiga yang tidak dapat dicegah meski telah dilakukan langkah-langkah keamanan maksimal.

Jika kita belajar dari Jepang melalui Act on the Protection of Personal Information (APPI) yang menerapkan pendekatan semi-strict liability, yang menggabungkan unsur preventif dan korektif. Seperti dalam kasus Mitsubishi UFJ Financial Group (MUFG), tanggung jawab hukum langsung diberlakukan setelah

 

terjadi pelanggaran data, dan regulator (FSA) secara otomatis memerintahkan audit, publikasi insiden, serta kompensasi kepada pihak terdampak. Pendekatan ini menunjukkan bahwa tanggung jawab otomatis mendorong kepatuhan dan transparansi, serta memperkuat kepercayaan publik terhadap sistem keuangan.

Dalam konteks Indonesia, penerapan strict liability atau setidaknya semi-strict liability akan lebih tepat diterapkan untuk perlindungan data perbankan, karena hal ini selaras dengan asas perlindungan konsumen sebagaimana diatur dalam UU No. 8 Tahun 1999, konsisten dengan semangat UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menempatkan pengendali data (dalam hal ini bank) sebagai pihak utama yang bertanggung jawab atas keamanan data, serta meningkatkan efektivitas penegakan hukum siber, yang saat ini masih lamban akibat sistem pembuktian berbasis kesalahan.

Dengan memperhatikan karakteristik sistem perbankan digital, tingkat kompleksitas teknologi, dan posisi lemah nasabah sebagai pengguna layanan, maka prinsip strict liability dinilai lebih tepat dan adil diterapkan dalam konteks perlindungan data perbankan dibandingkan dengan prinsip fault-based liability. Pendekatan ini tidak hanya menjamin keadilan substantif bagi nasabah, tetapi juga mendorong tanggung jawab preventif bagi bank untuk memastikan keamanan data nasabah secara berkelanjutan

## SIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa dalam kasus pelanggaran keamanan data perbankan di Indonesia, penerapan konsep Perbuatan Melawan Hukum (PMH) masih berlandaskan prinsip fault-based liability sebagaimana diatur dalam Pasal 1365 KUH Perdata. Konsekuensinya, tanggung jawab hukum baru dapat dikenakan apabila kesalahan pihak bank telah terbukti secara meyakinkan, sementara beban pembuktian masih berada pada nasabah sesuai Pasal 1865 KUH Perdata, yang pada praktiknya menyulitkan karena keterbatasan akses terhadap bukti teknis. Sebaliknya, hukum Jepang melalui Act on the Protection of Personal Information (APPI) menerapkan prinsip yang lebih progresif berupa semi-strict liability, di mana lembaga keuangan pada dasarnya dianggap bertanggung jawab atas pelanggaran data kecuali dapat membuktikan telah melakukan langkah pengamanan yang memadai. Dengan demikian, sistem hukum Jepang lebih berorientasi pada perlindungan konsumen dibandingkan sistem hukum Indonesia yang masih menitikberatkan pada pembuktian kesalahan.

Secara umum dapat disimpulkan pula bahwa perbedaan paradigma hukum tersebut menunjukkan orientasi kebijakan hukum yang berbeda: Jepang menempatkan perlindungan nasabah sebagai prioritas utama dengan menekankan tanggung jawab institusional bank atas pengelolaan data pribadi, sementara Indonesia masih berpegang pada prinsip pertanggungjawaban berbasis kesalahan individu. Oleh karena itu, sistem hukum Indonesia perlu memperkuat regulasi perlindungan data di sektor perbankan, mempertimbangkan penerapan prinsip tanggung jawab ketat atau semi-ketat, membangun mekanisme pengawasan terpadu antara OJK, Kominfo, dan Bank Indonesia, meningkatkan standar keamanan siber perbankan, menyediakan skema kompensasi yang cepat dan

 

transparan, serta memperkuat literasi digital dan pemahaman hukum masyarakat. Upaya kolaboratif antara regulator, industri perbankan, dan akademisi juga menjadi penting untuk mewujudkan tata kelola perlindungan data yang efektif, responsif, dan berkeadilan.

## DAFTAR RUJUKAN

Atmadja, W. S., G. D. Ginting, M. Q Dewani, J. M. Wijaya, and R. J. S. Pattiwael. 2025. "Journal of Social Research." *Fault-Based Liability vs. Strict Liability: Comparative Study of the Concept of Unlawful Acts Indonesia–Japan* 4 (10): 2973–2982.

R, Amalia. 2024. *Analisis Kebocoran Data Perbankan dalam Perspektif Hukum Perlindungan Konsumen. Jurnal Hukum dan Pembangunan Ekonomi* 9 (1): 55-72.

Repository Universitas Borneo Tarakan (UBT). 2025. "Kajian Implementasi UU PDP terhadap Sektor Perbankan Digital di Indonesia."

Irmawati, D., J. Rumondor, and M. Stoicov,. 2024. "Law and Digital Society Journal." *Legal and Technical Challenges in Data Protection Enforcement in Indonesian Banking Sector* 6 (2): 145–160.

Indonesia Business Post. 2023. "BSI's Data Breach: A Menace to Indonesia's Banking Security."

Reuters. 2024. "Japan Watchdog Recommends Action on MUFG Units Over Sharing Client Data."

Investing.com. 2024. "Japan Orders Compliance Improvements at MUFG Bank and Securities Tie-ups with Morgan Stanley."

The Japan Times. 2024. "Personal Info Leak Cases Hit Record High in Japan in Fiscal 2024."

Kitab Undang-Undang Hukum Perdata (KUHPerdata).

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

Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Surat Edaran Otoritas Jasa Keuangan (OJK) Nomor 14 Tahun 2024 tentang Penerapan Keamanan Data dan Informasi Sektor Jasa Keuangan.

Peraturan dan Dokumen Hukum (Jepang)

*Act on the Protection of Personal Information* (APPI) — Amendment 2020.

*Personal Information Protection Commission* (PPC Japan). *Guidelines on the Act on the Protection of Personal Information (General Rules)*, Tokyo, 2022