

ISSN (ONLINE) 2598 9928



INDONESIAN JOURNAL OF LAW AND ECONOMIC
PUBLISHED BY
UNIVERSITAS MUHAMMADIYAH SIDOARJO

Table Of Contents

Journal Cover	1
Author[s] Statement	3
Editorial Team	4
Article information	5
Check this article update (crossmark)	5
Check this article impact	5
Cite this article	5
Title page	6
Article Title	6
Author information	6
Abstract	6
Article content	7

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Copyright © Author(s). This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licences/by/4.0/legalcode>

EDITORIAL TEAM

Editor in Chief

Dr. Wisnu Panggah Setiyono, Universitas Muhammadiyah Sidoarjo, Indonesia ([Scopus](#)) ([Sinta](#))

Managing Editor

Rifqi Ridlo Phahlevy , Universitas Muhammadiyah Sidoarjo, Indonesia ([Scopus](#)) ([ORCID](#))

Editors

Noor Fatimah Mediawati, Universitas Muhammadiyah Sidoarjo, Indonesia ([Sinta](#))

Faizal Kurniawan, Universitas Airlangga, Indonesia ([Scopus](#))

M. Zulfa Aulia, Universitas Jambi, Indonesia ([Sinta](#))

Sri Budi Purwaningsih, Universitas Muhammadiyah Sidoarjo, Indonesia ([Sinta](#))

Emy Rosnawati, Universitas Muhammadiyah Sidoarjo, Indonesia ([Sinta](#))

Totok Wahyu Abadi, Universitas Muhammadiyah Sidoarjo, Indonesia ([Scopus](#))

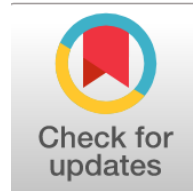
Complete list of editorial team ([link](#))

Complete list of indexing services for this journal ([link](#))

How to submit to this journal ([link](#))

Article information

Check this article update (crossmark)



Check this article impact (*)



Save this article to Mendeley



(*) Time for indexing process is various, depends on indexing database platform

Personal Data Protection in Banking Cybersecurity Breach Cases: Perlindungan Data Pribadi dalam Kasus Pelanggaran Keamanan Siber di Sektor Perbankan

Angelina Septiani Zaroh, sribudi@umsida.ac.id (*)

Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

Sri Budi Purwaningsih, sribudi@umsida.ac.id

Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

(*) Corresponding author

Abstract

General Background The rapid digitalization of banking services has increased the risk of cyber threats and unauthorized access to personal data. **Specific Background** Several cases of data breaches in Indonesian banking institutions highlight vulnerabilities in safeguarding customer information and raise concerns regarding legal protection mechanisms. **Knowledge Gap** However, limited studies analyze the legal responsibility of banks and the adequacy of personal data protection regulations in addressing such breaches. **Aims** This study aims to examine the legal framework governing personal data protection and analyze the accountability of banking institutions in cases of data breaches. **Results** The findings indicate that although regulations such as the Personal Data Protection Law provide a legal basis, challenges remain in enforcement and implementation, particularly in ensuring accountability and compensation for affected customers. **Novelty** This study emphasizes the relationship between cybersecurity incidents and legal liability within the Indonesian banking sector. **Implications** The results suggest the need for stronger regulatory enforcement and improved institutional compliance to ensure better protection of customer data in digital banking environments.

Keywords: Personal Data, Banking Security, Cybercrime, Legal Protection, Data Breach

Key Findings Highlights

Cyber incidents reveal weaknesses in institutional safeguards
Regulatory provisions exist but enforcement remains limited
Customer rights require stronger legal assurance

Published date: 2026-03-03

I. Pendahuluan

Data pribadi merupakan data berharga yang dimiliki oleh setiap orang. Data pribadi dikatakan sangat penting bagi setiap orang karena berisikan informasi yang akurat bagi pemilik data tersebut. Hal ini bersifat sangat sensitif sehingga harus dijaga kerahasiaannya dengan cermat oleh orang tersebut [1]. Dengan merahasiakan data pribadi dengan benar bertujuan untuk menjaga data pribadi secara optimal dan dapat mengantisipasi diri dari perbuatan orang-orang tidak bertanggung jawab yang mengatasnamakan data pribadi orang lain untuk kepentingan diri sendiri sehingga dapat melakukan perbuatan yang melawan hukum [2]. Sudah menjadi kewajiban negara Indonesia membuat Undang-Undang dengan tujuan melindungi data pribadi setiap warganya. Hal tersebut telah direalisasikan pada Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi yang di dalamnya menjelaskan bahwa data pribadi merupakan data tentang orang perorangan yang teridentifikasi atau diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik melalui sistem elektronik atau sistem non-elektronik [3].

Bank merupakan lembaga keuangan yang menghimpun dana dengan memberikan fasilitas kepada masyarakat dalam bentuk simpanan kemudian menyalurkan kembali kepada masyarakat dalam bentuk pinjaman yang bertujuan untuk meningkatkan taraf kehidupan masyarakat [4]. Menurut fungsinya Bank terbagi menjadi tiga bagian yakni Bank Sentra, Bank Umum dan Bank Perkreditan Rakyat. Dalam pengelompokannya, Bank terbagi lagi berdasarkan operasionalnya (Konvensional dan Syariah), kepemilikannya (Pemerintah, Swasta, Asing dan Campuran), dan terbagi lagi berdasarkan statusnya (Devisa dan Non-Devisa). Dari segala sisi pengelompokan dalam Bank satu hal yang pasti, kebijakan setiap Bank membutuhkan data pribadi dari setiap nasabah untuk bisa melakukan transaksi dan di mana data pribadi tersebut akan selalu menjadi kerahasiaan antar pihak. Meskipun sudah dibagi menjadi beberapa kategori dengan berbagai macam kebijakan di dalamnya, tidak semua Bank dapat menjamin dirinya sebagai lembaga keuangan yang aman untuk menjaga kerahasiaan nasabah, khususnya data pribadi yang dimiliki oleh nasabahnya.

Beberapa waktu yang lalu, lingkup perbankan diresahkan oleh perbuatan hacker yang melakukan peretasan pada sistem Bank. Kejadian ini terjadi pada salah satu Bank Pemerintah yang menyebabkan gangguan pada sistem layanan Bank. Peretasan yang dilakukan oleh sekelompok hacker Lock Bit 3.0 dengan menggunakan serangan ransomware berhasil mendapatkan data sekitar 1,5 TB dengan 15 juta data nasabah dan juga data karyawan Bank Tersebut [5]. Hal serupa juga terjadi pada salah satu Bank Swasta karena peretasan yang menyerang sistem dengan menggunakan sistem coding. Peretasan ini mengakibatkan beberapa nasabah mengeluh karena terdapat pengurangan jumlah saldo secara tiba-tiba tanpa melakukan transaksi apapun [6].

Dalam kejadian seperti ini secara tidak langsung berdampak pada nasabah yang menjadi korban dan mengalami kerugian baik secara materiil ataupun immaterial. Seharusnya Bank memberikan pertanggungjawaban kepada nasabah karena pihak Bank diberikan kepercayaan untuk menjamin keamanan dengan menjaga kerahasiaan mengenai data nasabah sesuai dengan aturan dalam Pasal 40 Ayat (1) Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan. Nasabah juga berhak untuk mendapatkan perlindungan terkait data pribadi sesuai dengan Pasal 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Namun, pada kejadian ini Bank mampu menepis dan memberikan pembelaan atas layanan Bank yang tidak berjalan dengan semestinya dan berdalih adanya pemeliharaan sistem yang mengakibatkan sistem tidak dapat digunakan dalam sementara waktu [7].

Terdapat dua penelitian terdahulu dengan membahas kasus yang serupa terkait perlindungan data pribadi. Penelitian pertama ditulis oleh Chaterine Grace Gunandi, Danisel Subrian, Elena Philomena Lee, Lauren Angel Gunawan dan Nichole Baretta dengan judul "Perlindungan Hukum Akibat Kebocoran Data Pribadi". Hasil dari penelitian ini mengkaji secara mendalam mengenai perlindungan hukum terhadap data pribadi [8]. Sedangkan penelitian ini berfokus pada analisis implementasi tentang bentuk perlindungan hukum terhadap nasabah Bank yang menjadi korban atas Ketidakamanan suatu sistem Bank dalam melakukan penyimpanan data pribadi nasabahnya. Penelitian kedua ditulis oleh I Gede Wahyu Yudistira dengan judul "Tanggung Jawab Hukum Bank Terhadap Kebocoran Data Nasabah Akibat Tindakan Peretasan Dalam Perspektif Hukum Positif Di Indonesia" [9]. Hasil dari penelitian ini menjelaskan terkait perlindungan data pribadi nasabah Bank dan bentuk tanggung jawab atas peretasan. Sedangkan penelitian ini menjelaskan pokok pembahasan lebih terperinci terlepas dengan adanya perlindungan hukum nasabah yang mengalami kebocoran data. Sedangkan penelitian ini juga menjabarkan apakah peristiwa kebocoran data pribadi yang dialami oleh nasabah termasuk dalam peristiwa hardship.

Penelitian ini bertujuan untuk menganalisis secara mendalam terkait peretasan yang terjadi pada lingkup perbankan. Selain itu, penelitian ini juga akan menjelaskan bahwa peretasan merupakan suatu tindak pidana yang mengakibatkan kerugian bagi para pihak terkait. Serta menjelaskan apakah kebocoran data pribadi akibat peretasan dapat dikategorikan sebagai hardship, overmacht atau force majeure

II. Metode

Penelitian ini menggunakan metode normatif dengan melakukan pendekatan perundang-undangan dan meneliti lebih dalam terkait Undang-Undang ITE Pasal 30 Ayat (1) dan Ayat (2) yang bisa dijadikan sebagai bahan hukum primer. Selain itu juga melakukan penelusuran melalui situs web, jurnal dan lain sebagainya untuk dijadikan sebagai bahan hukum sekunder.

III. Hasil dan Pembahasan

A. Peretasan Dalam Perbankan

Pada saat ini perkembangan ilmu pengetahuan terus berkembang. Tidak dapat dipungkiri kemajuan zaman berpengaruh pada kehidupan masyarakat, termasuk berpengaruh pada perkembangan ilmu pengetahuan dan teknologi yang semakin canggih dan mumpuni setiap kebutuhan manusia. Dapat dikatakan perkembangan ilmu pengetahuan dan teknologi memberikan dampak yang positif bagi kehidupan. Namun, sayangnya tidak semua dapat dimanfaatkan dengan bijaksana. Salah satunya yakni penyalahgunaan ilmu pengetahuan dan teknologi pada saat ini adalah tindakan peretasan [10]. Hal tersebut dibuktikan oleh peringkat Indonesia yang mengalami kenaikan dari peringkat 23 menjadi peringkat 5 sebagai negara yang paling banyak mengalami peretasan [11].

Peretasan didefinisikan sebagai suatu tindakan ilegal yang melanggar hukum dengan cara menerobos masuk secara paksa untuk mengakses sistem elektronik atau jaringan komputer orang lain yang bersifat pribadi dengan izin maupun tanpa izin. Pelaku peretasan disebut dengan hacker, hacker sendiri mampu meretas sejumlah situs web resmi milik negara misalnya melakukan peretasan atau pencurian data milik nasabah dalam perbankan. Dampak dari peretasan ini menimbulkan kerugian cukup besar baik itu materiil maupun immaterial. Berikut ini ada beberapa jenis peretasan yang biasa digunakan oleh hacker dalam melakukan tindak kejahatan, yakni :

1. Skimming

Skimming merupakan tindak kejahatan perbankan yang dilakukan dengan cara mencuri informasi data kartu ATM atau kartu kredit melalui skimmer [12]. Skimmer ialah alat yang biasanya dipasang pada lubang mulut ATM yang berguna untuk merekam data kartu atau bahkan PIN nasabah. Alat ini dapat menyimpan data kurang lebih 2000 kartu. Ada beberapa cara untuk mencegah terjadinya skimming, yakni :

a. Menghindari lokasi ATM yang sepi

Hal ini bertujuan untuk mengurangi resiko serangan skimming. Selain itu lokasi yang rawan biasanya dilengkapi dengan CCTV agar bisa memantau kegiatan orang lain yang mungkin akan melakukan tindak kejahatan skimming.

b. Memastikan ATM selalu dapat digunakan secara maksimal

Hal ini berguna untuk meyakinkan bahwa nasabah dapat melakukan transaksi dengan lancar, selain itu juga meningkatkan kepuasan nasabah saat melakukan transaksi melalui mesin ATM.

c. Mengganti kata sandi secara berkala

Mengganti sandi secara berkala bertujuan untuk mengantisipasi orang lain yang sudah mengetahui PIN ATM, penggantian PIN ATM sudah dihimbau oleh Bank guna mengantisipasi adanya peretasan.

d. Menggunakan kartu Chip-Based

Chip-Based bertujuan untuk meningkatkan keamanan dan efisiensi dalam melakukan transaksi. Data nasabah yang sudah tersimpan di dalamnya berkemungkinan kecil dapat digandakan. Maka dari itu, penggunaan Chip-Based lebih efisien digunakan oleh nasabah dalam melakukan transaksi perbankan.

2. Malware

Malware (Malicious software) merupakan suatu program yang sengaja dirancang dengan tujuan merusak. Arti merusak yang dimaksud yakni program ini secara khusus dirancang untuk menerobos atau menyusup secara paksa ke dalam sistem komputer mulai dari email, akses internet dan lain sebagainya [13]. Hal ini menyebabkan kerusakan pada beberapa sistem komputer yang mengakibatkan komputer berjalan lambat dalam merespons dan memungkinkan terjadinya pencurian data. Ada beberapa jenis malware yang perlu diketahui yakni :

a. Virus

Virus merupakan suatu program untuk mengidentifikasi komputer dan melumpuhkan perangkat. Penyebarannya dilakukan secara mandiri dari satu perangkat ke perangkat lain dengan tujuan untuk mencuri, menghapus atau mengambil alih.

b. Worm

Worm merupakan Malware yang secara otomatis dapat menginfeksi perangkat secara mandiri dengan cara menyebar melalui koneksi misal jaringan internet atau file yang terunduh.

c. Trojan Horse (Trojan)

Trojan merupakan Malware yang ditanam oleh aplikasi berbahaya. Tujuannya yakni untuk menginfeksi komputer dengan mencuri informasi sensitif dengan cara menyamar sebagai aplikasi yang terpercaya.

d. Adware

Adware biasanya menampilkan suatu iklan pop-up. Adware ini dapat masuk kedalam perangkat atau file secara tiba-tiba

dengan tujuan untuk mendapatkan penghasilan.

e.Spyware

Suatu Malware yang secara khusus dirancang untuk masuk kedalam perangkat untuk melakukan pengumpulan data dan mengirim pada pihak ketiga tanpa sepengetahuan pengguna.

f.Ransomware

Ransomware penyebarannya melalui tautan yang secara otomatis dapat mengunci sistem korban dengan tujuan meminta tebusan kepada korban dengan menjadikan data tersebut sebagai jaminan.

g.Botnet

Botnet dapat ditanam melalui Trojan atau malware lainnya dengan melakukan serangan siber seperti DDoS, phishing dan serangan lainnya.

Ada beberapa cara untuk mengatasinya, yakni :

a.Melakukan pencadangan data pribadi agar tetap aman,

b.Menggunakan software anti malware supaya meminimalisir adanya peretasan

c.Lebih berhati-hati ketika menginstal atau mengupdate sistem pada perangkat yang menggunakan jaringan internet

3.Hacking

Hacking merupakan suatu kegiatan yang menyerang program komputer. Berbeda dengan malware yang merancang sistem, hacking berfokus pada kegiatan menyusup pada sistem atau program milik orang lain dengan memanfaatkan kerentanan atau keamanan sistem yang lemah pada perangkat lunak atau menggunakan teknik Social Engineering untuk memanipulasi data milik orang lain. Ada beberapa jenis hacking yang perlu kita ketahui, yakni :

a.Malicious hacking (Black Hat)

Black hat merupakan aktivitas hacking yang dilakukan dengan memaksa yang bertujuan untuk mencuri data sensitif dan menguntungkan diri sendiri.

b.Ethical hacking (White Hat)

White hat merupakan aktivitas hacking yang dilakukan secara resmi dengan diizinkan untuk meningkatkan keamanan suatu sistem dan dapat memberikan peringatan ketika terdapat suatu sistem yang lemah.

c.Grey hat hacking

Grey hat merupakan jenis hacking campuran, karena tidak sepenuhnya jahat dan tidak sepenuhnya baik. Penyebarannya melalui kerentanan suatu perangkat tanpa adanya izin resmi dengan tujuan untuk meningkatkan keamanan sistem. Namun, tidak selalu digunakan untuk keuntungan pribadi.

Ada beberapa cara untuk mengatasinya, yakni :

a.Menggunakan anti virus dengan kualitas yang terbaik.

b.Selalu mengupgrade sistem untuk menghindari peretasan akibat kelemahan sistem.

c.Selalu menggunakan VPN saat mengakses jaringan internet.

d.Menggunakan password manager untuk mengatur password.

Secara menyeluruh tidak dapat dibenarkan terkait adanya peretasan, karena hal tersebut dilakukan dengan sengaja dan melawan hukum. Sama seperti salah satu contoh kasus yang terjadi pada salah satu bank, dimana bank tersebut diidentifikasi mendapat serangan hacker berjenis ransomware dengan melakukan ancaman dan akan menyebarluaskan data sebesar 1,5 TB. Namun untungnya Bank tersebut memberikan respon dengan cepat terkait peristiwa yang terjadi pada instansinya, selain itu pihak Bank berhasil untuk meyakinkan bahwa hal tersebut bukan merupakan peretasan melainkan adanya pemeliharaan sistem.

Peretasan sudah diatur dalam Pasal 30 Ayat (1) UU ITE yang berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas sistem informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain" dan juga Pasal 30 Ayat (2) UU ITE yang berbunyi : "Setiap orang yang sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi

elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan". [14].

Tidak dapat dianggap remeh, karena pelaku peretasan akan mendapatkan sanksi sesuai dengan Pasal 47 UU ITE "setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau Ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah)".

B. Keterkaitan Transaksi Elektronik Dengan Adanya Peretasan

Transaksi elektronik didefinisikan sebagai perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan dan media elektronik dengan memanfaatkan jaringan internet. Transaksi elektronik dapat dilakukan dengan cara mengumpulkan data, menyiapkan, menganalisis dan menyebarkan. Semakin berkembangnya teknologi elektronik, Bank juga menyediakan jasa pelayanan yang memudahkan nasabahnya melakukan transaksi dengan mudah melalui media elektronik. Hal tersebut didukung dengan adanya Pasal 5 Ayat (1) Undang-Undang ITE yang berbunyi "Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah" [15]. Dengan artian bahwa transaksi elektronik dapat dikatakan sah apabila dilakukan sesuai dengan ketentuan yang sudah diberlakukan.

Namun, selain Bank menyediakan jasa transaksi elektronik yang memudahkan nasabahnya, transaksi elektronik mempunyai kekurangan, berikut ini beberapa contoh negatif adanya transaksi elektronik pada Bank :

1. Penyalahgunaan data

Data yang disimpan dengan rapi pada sistem Bank, tidak memberikan jaminan akan selalu aman kerahasiaannya. Hal tersebut bisa jadi disalahgunakan oleh orang yang tidak bertanggung jawab untuk melakukan transaksi ilegal. Pelaku tersebut dapat melakukannya dengan cara mengakses nomor kartu kredit milik nasabah bahkan juga PIN melalui internet Banking atau aplikasi Mobile banking.

2. Adanya kerusakan sistem

Serangan cyber dapat berhasil masuk dengan membobol sistem pada perangkat bank. Dengan begitu dapat mengganggu operasional perbankan dan menyebabkan kerugian. Penggunaan internet banking tidak dapat dikatakan efisien, karena nasabah harus berhati-hati dalam menjaga data pribadi mereka dan menggunakan teknologi yang aman dan memadai untuk menjaga data pribadi mereka.

Maka dari itu, penyelenggara sistem berperan penting untuk memastikan keamanan data sesuai dengan aturan hukum yang berlaku yaitu Pasal 27 Tahun 2022 Tentang Perlindungan Data Pribadi dan bertanggung jawab jika terjadi peretasan pada sistem yang dioperasikan sesuai dengan Pasal 26 ayat (2) Undang-Undang ITE.

C. Teori Hardship, Force Majeure dan Overmatch

1. Hardship

Hardship diartikan dalam bahasa Indonesia yakni keadaan sulit atau kesulitan. Istilah ini dikenal secara luas karena adanya praktik perdagangan internasional. Hardship biasanya digunakan ketika terjadi suatu peristiwa yang tidak dapat diperkirakan sebelumnya. Dalam kontrak, peristiwa ini berisiko karena berubahnya keseimbangan perjanjian secara mendasar, karena meningkatnya biaya pelaksanaan perjanjian sehingga dapat membebani debitur atau juga sebaliknya menghilangkan keuntungan bagi kreditur [16]. Karakteristik hardship dalam hukum kontrak yaitu :

a. Perubahan kondisi fundamental

Hardship dapat terjadi ketika perubahan kondisi secara fundamental mengganggu keseimbangan kontrak. Misalnya seperti perubahan nilai kontrak yang sangat tinggi atau rendah.

b. Keseimbangan kontrak

Hardship dapat mempengaruhi keseimbangan kontrak sehingga pihak yang dirugikan harus melaksanakan kontrak dengan tindak pada ketentuan tentang pelaksanaan kontrak yang cukup penting.

c. Sifat mengikat

Meskipun kontrak menyebabkan kesulitan bagi salah satu pihak atau kedua nya, kontrak harus tetap dilaksanakan karena bersifat mengikat.

d. Akomodatif dan fleksibel

Hardship dianggap lebih akomodatif dan fleksibel sehingga dapat menyelesaikan kasus yang memiliki karakteristik keadaan yang mempengaruhi keseimbangan kontrak.

e. Pengaturan dalam klausul

Hardship sering diatur dalam klausul sebagai salah satu metode alternatif untuk menyelesaikan kasus. Karena dianggap dapat memberikan solusi saat sengketa.

Meskipun hardship belum diatur secara resmi dalam Undang-Undang Dasar atau Undang-Undang Hukum Perdata, penyelesaian kasus Hardship di pengadilan biasanya menggunakan teori force majeure. Jika diterapkan dalam lingkup perbankan, bank mengalami suatu kesulitan karena adanya peretasan yang tidak dapat diduga sebelumnya, maka bank menggunakan teori hardship untuk menuntut renegotiasi perjanjian atau meminta bantuan pada pihak berwenang untuk mengatasi permasalahannya.

Teori hardship terkait dengan peretasan pada Bank dapat dilihat dalam beberapa aspek yang terakit sebagai berikut:

a. Kebocoran data: Peretasan dalam Bank menyebabkan kebocoran data nasabah yang menimbulkan dampak yang merugikan seperti terjadinya penipuan, pencurian data pribadi, hingga penyalahgunaan finansial.

b. Strategi Penolakan (Denial): Pada awalnya Bank tersebut menyangkal adanya peretasan disebabkan karena adanya gangguan, mengklaim bahwa disebabkan adanya pemeliharaan sistem. Namun pada akhirnya memberikan pernyataan bahwa adanya gangguan disebabkan oleh serangan ransomware.

c. Krisis Komunikasi: Peretasan yang terjadi pada Bank tersebut dapat memicu adanya krisis komunikasi, di mana pihak Bank harus menghadapi kepercayaan publik yang terganggu dan reputasi Bank menjadi terancam.

d. Keseluruhan Dampak: Secara keseluruhan adanya peretasan yang terjadi pada Bank secara tidak langsung mengancam kepercayaan nasabah terhadap institusi perbankan lainnya. Bank harus mengambil langkah serius untuk bisa memulihkan reputasi dan mengembalikan pelayanan publik.

Namun demikian, adanya peretasan pada Bank yang menyebabkan kebocoran data pribadi nasabah tidak dapat dikatakan hardship. Karena sudah menjadi tanggung jawab Bank untuk menjaga keamanan sistem dan meyakinkan nasabah bahwa data pribadinya tetap aman meskipun peretasan pada Bank tidak dapat dihindari.

2. Force Majeure dan Overmacht

Force majeure dan overmatch memiliki arti yang sama dalam bahasa Indonesia yakni keadaan memaksa. Dalam suatu perjanjian, istilah ini digunakan untuk melindungi pihak yang tidak dapat memenuhi prestasi namun tidak dapat dinyatakan sebagai perbuatan wanprestasi [17]. Overmacht dan force majeure diatur dalam pasal yang sama yakni pasal 1244 dan 1245 KUHPerdata. Dimana Pasal tersebut berisikan bahwa keadaan memaksa terjadi apabila debitur terhalang untuk memenuhi prestasinya karena suatu keadaan yang tidak dapat diduga dan tidak dapat diberikan pertanggungjawaban, maka debitur dibebaskan dalam biaya ganti rugi dan bunga.

Pada lingkup perbankan, bilamana bank mengalami keadaan memaksa akibat peretasan yang berdampak tidak terpenuhinya prestasi, maka bank dapat menjadikan teori force majeure dan overmatch untuk meminta pembebasan dari kewajiban ketika peristiwa ini berlangsung. Namun Bank tidak dapat dikatakan sebagai pihak yang melanggar wanprestasi karena peristiwa ini (peretasan) merupakan keadaan memaksa dan di luar kendali bank. Berikut ini perbedaan karakteristik antara force majeure dan overmatch yaitu :

a. Kondisi mendesak

- Force majeure : Merupakan situasi mendesak yang tidak dapat dikendalikan (bencana alam, perang atau pandemi).
- Overmacht : Merupakan situasi mendesak yang tidak dapat dikendalikan, tetapi lebih luas dan tidak membatasi objek pembahasan.

b. Kewajiban debitur

- Force majeure : Debitur tidak dapat memenuhi kewajiban karena keadaan tersebut.
- Overmacht : Debitur tidak dapat memenuhi kewajiban karena keadaan tersebut. Tetapi tidak dapat di salahkan dan tidak harus menanggung risiko.

c. Penangguhan sementara

- Force majeure: Memberikan penangguhan sementara pada debitur untuk melakukan kewajiban setelah peristiwa.
- Overmacht : Memberikan penangguhan sementara, tetapi dengan syarat bahwa debitur tidak dapat di salahkan dan tidak harus menanggung risiko.

d. Dasar hukum

Dasar hukum force majeure dan overmatch diatur dalam Pasal 1244 dan 1245 KUHPerdara

e. Penggantian biaya

Penggantian biaya, ganti rugi dan bunga dapat di maafkan jika keadaan tersebut memaksa, tetapi dengan syarat debitur tidak dapat di salahkan.

f. Kriteria

Force majeure dan overmatch sama-sama dalam keadaan yang memaksa dan harus benar-benar mengakibatkan prestasi tidak dapat di laksanakan.

g. Kedudukan dalam hukum

• Force majeure : Dalam hukum perdata, force majeure diatur sebagai salah satu alasan untuk tidak memenuhi kewajiban kontrak.

• Overmacht : Dalam hukum perdata, overmatch juga diatur sebagai salah satu tidak memenuhi kewajiban dalam kontrak, namun hal ini bersifat lebih luas.

Force majeure dan overmatch dalam kasus peretasan pada Bank dapat merujuk pada aspek pembelaan . Karena adanya peretasan pada sistem bank merupakan keadaan yang tidak terduga atau dapat di prediksi sebelumnya. Meskipun demikian, Bank tetap harus melakukan ganti rugi pada nasabah yang merasa menjadi korban karena peretasan. Meskipun demikian peretasan tidak dapat dibantah, walaupun Bank tidak menjelaskan secara mendetail dan sudah semestinya Bank bertanggung jawab atas peretasan yang terjadi pada sistemnya. Karena peretasan dapat terjadi akibat keamanan sistem Bank yang mudah untuk di retas dan hal tersebut merupakan kelalaian dari Bank dalam menjaga data pribadi nasabahnya.

VII. Simpulan

Berdasarkan pembahasan di atas dapat disimpulkan bahwa peretasan merupakan suatu perbuatan yang melawan hukum karena menggunakan akses ilegal pada sistem milik orang lain dan hal tersebut sudah jelas tercantum dalam Pasal 30 UU ITE. Peretasan yang terjadi baik dalam lingkup perbankan atau tidak merupakan peristiwa yang tidak terduga atau tidak dapat diprediksi oleh pihak terkait. Namun hal tersebut tidak dapat dikatakan sebagai hardship, force majeure ataupun overmatch meskipun termasuk ke dalam keadaan sulit yang tidak dapat diperkirakan sebelumnya dan dapat disimpulkan bahwa kebocoran data pribadi tidak dapat di kategorikan sebagai hardship karena sudah semestinya Bank bertanggung jawab kepada nasabah karena pihak Bank diberikan kepercayaan untuk menjamin keamanan dengan menjaga kerahasiaan mengenai data nasabah sesuai dengan aturan dalam Pasal 40 Ayat(1) Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan.

Ucapan Terima Kasih

Alhamdulillah, saya panjatkan syukur kepada Allah SWT karena dengan rahmat-Nya saya dapat menyelesaikan tugas akhir saya dengan lancar dan tepat waktu. Tidak lupa juga Saya ucapkan terima kasih kepada Universitas Muhammadiyah Sidoarjo karena telah memberikan fasilitas yang lebih dari cukup untuk Saya sebagai mahasiswa dapat mengerjakan tugas akhir ini dan terakhir saya ucapkan terima kasih untuk diri saya sendiri karena sudah bisa bertahan sampai di titik ini. Semoga bantuan dan dukungan yang diberikan kepada saya dapat menjadi amal jariyah dan semoga juga Allah SWT selalu melimpahkan rahmat dan berkat-Nya kepada kita semua.

References

1. A. D. Artija and S. B. Purwaningsih, "Legal Protection for Holders of Unused Foreign Brands in Terms of the First to File Principle in Indonesia," UMSIDA Preprints, Sep. 2023, doi: 10.21070/ups.3271.
2. S. A. Kusnadi, "Legal Protection of Personal Data as Privacy Rights," Al Wasath Journal of Law, vol. 2, no. 1, Apr. 2021, doi: 10.47776/alwasath.v2i1.127.
3. Republic of Indonesia, "Law No. 27 of 2022 on Personal Data Protection," 2022.
4. Republic of Indonesia, "Law No. 10 of 1998 on Banking," 1998.
5. N. Maulana et al., "Crisis Management of PT BSI Tbk After Data Breach," Innovative Journal of Social Science Research, vol. 4, no. 1, Feb. 2024, doi: 10.31004/innovative.v4i1.8620.
6. G. Mediatama, "Reviewing BSI Case and Banking Data Breaches," Kontan, 2024.
7. Z. Aprilia, "Bank Account Breach Case Analysis," CNBC Indonesia, 2023.
8. C. G. Gunadi et al., "Legal Protection on Personal Data Breach," Conference on Law and Social Studies, vol. 4, no. 1, Nov. 2023.
9. T. Lestari et al., "Banking Liability in Protecting Customer Data," Jurnal Dunia Ilmu Hukum dan Politik, vol. 2, no. 3, May 2024, doi: 10.59581/doktrin.v2i3.3202.
10. S. Anissa and M. T. Multazam, "Law Enforcement Mechanisms for Personal Data Abuse," UMSIDA Preprints, Aug. 2023, doi: 10.21070/ups.2852.
11. R. Fachrizal, "Indonesia Ranked Fifth in Global Cyberattacks," InfoKomputer, 2024.
12. E. F. Hidayati, "Validity of Electronic Evidence in Civil Trials," 2024.

Indonesian Journal of Law and Economics Review

Vol. 21 No. 1 (2026): February

DOI: 10.21070/ijler.v21i1.1533

13. M. K. Faridi, "Cybercrime in Banking Sector," *Cyber Security dan Forensik Digital*, vol. 1, no. 2, Mar. 2019, doi: 10.14421/csecurity.2018.1.2.1373.
14. Republic of Indonesia, "Law No. 19 of 2016 on Electronic Information and Transactions," 2016.
15. D. J. Rasuh, "Force Majeure in Civil Law," *Lex Privatum*, vol. 4, no. 2, Feb. 2016.
16. K. A. Kusuma, "Hardship Clause in Unidroit Principles," Undergraduate thesis, Universitas Airlangga, 2009.
17. S. Rokoyah and N. F. Mediawati, "Insurance Claims Related to War Risk," *UMSIDA Preprints*, Aug. 2023, doi: 10.21070/ups.3048.