Science and Education Journal
Vol 5 No 2 (2026)
E-ISSN : 2962-9713
P-ISSN : 2963-928X

Analisis Yuridis Perlindungan Hukum Nasabah Bank Dalam Hal Terjadinya Tindak Pidana *Illegal Access* Dan Manipulasi Data

Muhammad Hilman[1], Margo Hadi Pura[2], Taryani kesumawardani[3]
[1]Universitas Singaperbangsa Karawang, hilmanmuhammad142004@gmail.com
[2]Universitas Singaperbangsa Karawang,margo.hadi@fh.unsika.ac.id
[3]Universitas Singaperbangsa Karawang, taryanikesumawardani@gmail.com

Abstrak

Pentingnya perlindungan hukum ketika nasabah menghadapi ancaman siber menjadi alasan diperlukannya penelitian forensik yang mendalam. Penelitian ini bertujuan untuk mengetahui perlindungan hukum yang diberikan kepada nasabah bank apabila terjadi tindak pidana pelanggaran hukum akses dan manipulasi data. Dengan menganalisis undang-undang, peraturan, dan praktik yang relevan, penelitian ini diharapkan dapat berkontribusi dalam memperkuat perlindungan hukum nasabah bank di Indonesia. Penelitian ini menggunakan penelitian hukum normatif, yang menekankan pada studi dokumen dalam penelitian kepustakaan untuk mempelajari data sekunder di bidang hukum yang berhubungan dengan permasalahan dan tujuan penelitian ini. Pendekatan yang digunakan adalah pendekatan konseptual dan pendekatan historis. Pengaturan tindak pidana terhadap pelaku pengaksesan ilegal dan manipulasi data kepada nasabah bank jelas diatur pada Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-undang No 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Tindak pidana dalam perbankan merupakan masalah hukum yang mempengaruhi sektor perbankan dan kerangka hukum. Dewan Eropa - Konvensi Kejahatan Siber (ETS No. 185) menekankan perlunya undang-undang yang lebih ketat untuk mencegah manipulasi data ilegal. Tindakan ini juga membantu dalam mencegah akses ilegal dan bentuk kejahatan dunia maya lainnya.
Kata kunci: *Perlindungan hukum, Illegal access, nasabah bank.*

Abstract

The importance of legal protection when customers face cyber threats is the reason for the need for in-depth forensic research. This study aims to determine the legal protection provided to bank customers in the event of criminal acts of violating the law, access and manipulation of data. By analyzing relevant laws, regulations, and practices, this research is expected to contribute to strengthening the legal protection of bank customers in Indonesia. This study uses normative legal research, which emphasizes the study of documents in literature research to study secondary data in the field of law related to the problems and objectives of this research. The approach used is a conceptual approach and a historical approach. The regulation of criminal acts against perpetrators of illegal access and manipulation of data to bank customers is clearly regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) and Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). Criminal acts in banking are legal issues that affect the banking sector and the legal framework. Council of Europe – The Cybercrime Convention (ETS No. 185) emphasizes the need for stricter legislation to prevent illegal data manipulation. This action also helps in preventing illegal access and other forms of cybercrime.
Keywords: *Legal protection, Illegal access, bank customers*

Corresponding Author:
Muhammad Hilman
Universitas Singaperbangsa Karawang, hilmanmuhammad142004@gmail.com

E-ISSN : 2962-9713
P-ISSN : 2963-928X

PENDAHULUAN

Selama beberapa dekade terakhir, pesatnya perkembangan teknologi informasi memberikan dampak yang signifikan terhadap industri perbankan. Digitalisasi layanan perbankan membuat produk dan layanan keuangan lebih mudah diakses oleh nasabah. Namun di sisi lain, kemajuan ini juga meningkatkan risiko terhadap keamanan data pelanggan, terutama ancaman kejahatan dunia maya seperti akses ilegal dan manipulasi data. Akses ilegal ini tidak hanya mengancam keamanan data nasabah, tetapi juga merusak stabilitas sistem perbankan dan merusak kepercayaan masyarakat terhadap lembaga keuangan.

Illegal access adalah kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sitem jaringan komputer secara tidak sah, tanpa ijin atau tanpa sepengetahuan dari pemilik system jaringan computer yang dimasukinya. Biasanya pelaku melakukan dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Tindakan illegal access tersebut juga termasuk dalam ranah tindak terlarang cybercrime, yakni bentuk tindak kejahatan yang memanfaatkan teknologi komputer, jaringan komputer, internet atau perangkat digital lainnya sebagai alat, sasaran, tempat atau penggunanya.[1]

Peran teknologi informasi, media, komunikasi dan sistem elektronik sangat bermanfaat bagi perubahan perilaku masyarakat secara global. Sistem elektronik yang dimaksud yaitu perangkat keras, perangkat lunak komputer, jaringan telekomunikasi dan sistem komunikasi elektronik.[2] Dalam dunia maya, semua data baik berupa tulisan, gambar bahkan video tidak akan pernah bisa dihapus secara permanen, dan hal ini disebut sebagai rekam jejak digital, dimana dari pengunggahan tersebut meninggalkan jejak yang kemudian masih bisa ditelusuri informasinya. Tentu hal ini sangat berbahaya apabila tidak diberikan perlindungan yang baik dalam rangka menghindari terjadinya akses ilegal yang dilakukan oleh oknum atas data pribadi yang telah diunggah.

Tindak pidana akses ilegal dan manipulasi data merupakan salah satu permasalahan hukum yang perlu segera diselesaikan. Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan berbagai peraturan Otoritas Jasa Keuangan (OJK), Pemerintah Indonesia telah memberlakukan peraturan untuk melindungi data nasabah dan membakukan sanksi terhadap pelaku kejahatan dunia maya di sektor perbankan. Namun, peraturan yang ada masih dianggap belum cukup untuk mengekang semakin parahnya kejahatan dunia maya dan tidak cukup menjamin perlindungan hukum bagi nasabah.

Pentingnya perlindungan hukum ketika nasabah menghadapi ancaman siber menjadi alasan diperlukannya penelitian forensik yang mendalam. Penelitian ini bertujuan untuk mengetahui perlindungan hukum yang diberikan kepada nasabah bank apabila terjadi tindak pidana pelanggaran hukum akses dan manipulasi data. Dengan menganalisis undang-undang, peraturan, dan praktik yang relevan, penelitian ini diharapkan dapat berkontribusi dalam memperkuat perlindungan hukum nasabah bank di Indonesia.

Ancaman akses ilegal dan manipulasi data menjadi sebuah masalah, salah satunya terjadi pada PT. Bank Central Asia Tbk. Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Metro Jaya menetapkan seorang tersangka pembocoran sekaligus 20.000 data manipulasi nasabah PT Bank Central Asia Tbk. atau BCA sekitar tahun

[1] https://www.kajianpustaka.com
[2] Bala Tim PY, Undang-Undang Informasi Dan Transaksi Elektronik: Seri Perundangundangan (Yogyakarta: Pustaka Yustisia, 2019), hal 33–34.

E-ISSN : 2962-9713
P-ISSN : 2963-928X

2023.[3] Hal ini dapat menjadi bukti bahwasannya masih banyak sekali ketidaksesuaian dan maraknya ancaman kejahatan bahkan dalam sektor dunia maya seperti akses ilegal dan manipulasi data. Kasus ini menjadi tolak ukur agar nasabah dapat berhati-hati dalam menggunakan dan menyebarluaskan data yang bersifat rahasia, karena kejahatan oknum siber tidak dapat diterka. Dengan demikian, sepatutnya nasabah juga perlu untuk menjaga kerahasiaan dari data-data pribadinya secara seksama meski negara sudah menjaminkan mengenai perlindungan setiap data pribadi termasuk data dari nasbah bank melalu Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi agar tidak ada peluang terjadinya kejahatan akses ilegal dan manipulasi data.

METODE

Dalam melakukan suatu penelitian ilmiah jelas harus menggunakan metode sebagai ciri khas keilmuan Metode mengandung makna sebagai cara mencari informasi dengan terencana dan sistimatis. Langkah-langkah yang diambil harus jelas serta ada batasanbatasan yang tegas guna menghindari terjadinya penafsiran yang terlalu luas.[4] Penelitian ini menggunakan penelitian hukum normatif, yang menekankan pada studi dokumen dalam penelitian kepustakaan untuk mempelajari data sekunder di bidang hukum yang berhubungan dengan permasalahan dan tujuan penelitian ini. Pendekatan yang digunakan adalah pendekatan konseptual dan pendekatan historis.[5]

HASIL DAN PEMBAHASAN

1. Bentuk tanggung jawab hukum yang dapat dikenakan kepada pihak yang melakukan tindak pidana Illegal Access dan manipulasi data terhadap nasabah bank

Perkembangan zaman saat ini semakin cepat begitupun yang terjadi pada perkembangan teknologi. Saat ini teknologi memiliki peran penting dalam kehidupan manusia, seakan-akan teknologi sudah mulai menjadi kebutuhan primer dimana hal itu sangat penting dan harus selalu ada untuk kelangsungan hidup manusia. Namun, pada realitanya kondisi penggunaan teknologi tidak hanya bersifat positif sebagai sarana pendukung kebutuhan hidup sehari-hari manusia akan tetapi banyak terjadi penyalahgunaan teknologi terutama pada sektor perbankan. Digitalisasi yang semakin maju pada layanan perbankan dapat memudahkan nasabah bank dalam mengakses data yang dimilikinya, akan tetapi hal tersebut tidak terlepas pada ancaman risiko terjadinya pencurian, penipuan atau bahkan manipulasi data pribati nasabah bank. Ancaman keaman yang marak terjadi tidak hanya menimbulkan kekhawatiran bagi nasabah akan tetapi bagi sistem perbankan.

Secara umum tindak pidana di bidang perbankan adalah suatu perbuatan yang melanggar ketentuan yang diatur dalam undang-undang perbankan maupun yang terdapat dalam ketentuan pidana sedangkanga istilah kejahatan di bidang perbankan merupakan perbuatan yang dilakukan terkait industri perbankan yang menyalahi aturan hokum yang bisa melibatkan pihak perbankan maupun nasabahnya baik sebagai pelaku maupun korban. Padahal pengaturan terkait tindak pidana di bidang perbankan seperti pencurian uang, pemalsuan dokumen nasabah, pemusnahan pelaporan dan yang saat ini marak terjadi seperti akses ilegal serta manipulasi data memang didalamnya telah jelas

[3] Deny Saputra, *Polri Ungkap Motif Pelaku 'Manipulasi' Data Nasabah BCA*, Kabar 24, Agustus 2023.
[4] Soerjono Soekanto dan Sri Mamudi, 1986, Penelitian Hukum Normatif, (Jakarta: CV. Rajawali), hal. 27
[5] Muh. Alfian, *Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan,* JURNAL KOSMIK HUKUM Vol. 17 No. 2 Juni 2017, hlm. 150-151

E-ISSN : 2962-9713
P-ISSN : 2963-928X

diterangkan dalam Undang-Undang Nomor 10 Tahun 1998 tentang perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan yang (selanjutnya disebut UU Perbankan).[6] Akan tetapi pengaturan lebih lengkap mengenai tindak pidana akses ilegal dan manipulasi data tertuang pada Pasal 2 Konvensi tentang Tindak Pidana Telematika atau *Council of Europe - Convention on Cybercrime* (ETS No. 185) menyatakan bahwa setiap negara harus menerapkan langkah-langkah hukum dan lain-lain yang diperlukan untuk menjadikan akses tanpa hak ke sistem komputer sebagai kejahatan pidana. Konvensi tentang tindak pidana telematika atau *Council of Europe - Convention on Cybercrime* mengaruskan kepada setiap negara untuk menerapkan Undang-undang untuk tindakan pidana akses ilegal.[7]

Teknologi informatika saat ini telah menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum, dengan kata lain terjadinya perbuatan-perbuatan melawan hukum tersebut maka ruang lingkup hukum harus diperluas untuk menjangkau perbuatan-perbuatan tersebut. Dampak negatif selain kemudahan dan kenyamanan layanan internet itu, ada ancaman yang sangat merisaukan, yakni sisi keamanannya. Pengamanan sistem informasi berbasis internet perlu diperhatikan, karena jaringan informasi yang bersifat publik dan global sangat rentan dari berbagai bentuk kejahatan. Ancaman timbul manakala seseorang mempunyai keinginan memperoleh akses ilegal ke dalam jaringan komputer, sehingga lahirlah perilaku-perilaku me nyimpang dengan memanfaatkan teknologi canggih sebagai alat untuk mencapai tujuan dengan melakukan kejahatan. Kejahatan-kejahatan ini dikenal sebagai kejahatan dunia maya atau cyber crime.[8]

Pengaturan tindak pidana terhadap pelaku pengaksesan ilegal dan manipulasi data kepada nasabah bank jelas diatur pada Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-undang No 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dengan demikian dalam hal terjadinya tindakan akses ilegal dan manipulasi data pada data pribadi nasabah bank, pelaku dapat dikenakan berbagai sanksi yang sudah diatur oleh Undang-undang terkait.

Pasal 66 Undang-undang tentang Perlindungan Data Pribadi menyatakan: *Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.* Larangan tersebut sudah jelas diatur pada Undang-undang, dengan demikian apabila seseorang melakukan tindakan mengakses data pribadi seseorang dengan tidak memiliki hak dapat dianggap sebagai tindakan melawan hukum yang harus mendapatkan pertanggung jawaban bagi pelaku karena sudah merugiakan banyak pihak baik nasabah bank, lembaga keuangan maupun pihak lain yang terlibat.

Dengan demikian, sebagai pertanggungjawaban serta perlindungan hukum, pelaku tindak pidana Illegal Access dan manipulasi data terhadap nasabah bank dapat dikenakan berbagai bentuk tanggung jawab hukum. Berdasarkan Pasal 67 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pelaku dapat dijatuhi pidana penjara maksimal 6 (enam) tahun. Selain itu, pelaku juga dapat dikenakan pidana denda

[6] Galang Ramadhan Djokdja, dkk. *Pertanggungjawaban Pidana Pelaku Pembobolan Kartu Kredit Dalam Tindak Pidana Di Bidang Perbankan.* TATOHI Jurnal Ilmu Hukum Vol 2, No 2 (2022), Hal. 179

[7] Seri perjanjian eropa 185 – Konvensi Tentang Tindak Pidana Telematika, Budapest, 23.IX.2001.

[8] Rezy Januar Wilyana, Imam Budi Santoso, and Oci Senjaya, "Pembuktian Bukti Elektronik Di Persidangan," Singaperbangsa Law Review 1, no. 1 (2020): 164–83.

E-ISSN : 2962-9713
P-ISSN : 2963-928X

hingga Rp 6.000.000.000 (enam miliar rupiah). Hukuman ini bertujuan memberikan efek jera bagi pelaku dan melindungi hak-hak nasabah yang dirugikan akibat tindakan tersebut. Tidak hanya itu, pelaku juga dapat dimintai tanggung jawab secara perdata apabila tindakannya menyebabkan kerugian materiil maupun immateriil pada nasabah. Nasabah yang dirugikan berhak mengajukan gugatan ganti rugi atas pelanggaran data pribadinya. Jika pelaku merupakan badan usaha atau korporasi, selain pidana, mereka juga dapat dikenakan sanksi administratif sebagaimana diatur dalam Pasal 55 hingga Pasal 62 UU PDP. Sanksi administratif ini dapat berupa peringatan tertulis, denda administratif, penghentian sementara aktivitas pemrosesan data, hingga pencabutan izin usaha.

Selain aturan dalam UU PDP, tindakan Illegal Access juga diatur dalam Pasal 30 Undang-Undang No. 19 Tahun 2016 tentang Perubahan UU ITE, yang mengancam pelaku dengan pidana penjara maksimal 6 (enam) tahun dan/atau denda hingga Rp 600 juta. Dengan berbagai ketentuan tersebut, pelaku tindak pidana yang melanggar privasi data nasabah menghadapi kombinasi sanksi pidana, perdata, dan administratif yang bertujuan untuk menegakkan keadilan serta melindungi data pribadi masyarakat.

2. Perlindungan Hukum Nasabah Bank dalam Hal Terjadinya Tindak Pidana Illegal Access dan Manipulasi Data

Perkembangan jaman yang semakin kompleks dan dinamis seperti sekarang ini tidak dapat di pungkiri bahwa tekhnologi dan internet semakin berkembang pesat, hampir setiap saat kegiatan yang kita lakukan selalu berhubungan dengan yang namanya tekhnologi dan internet. Bukan hanya untuk hiburan, internet juga kini bisa digunakan menjadi salah satu media belanja, pembelajaran, pekerjaan dan banyak hal lainnya. Dengan kebutuhan yang semakin kompleks dan internet mempermudah semua hal itu, maka internet menjadi kebutuhan manusia yang tidak bisa dipisahkan lagi. [9]

Saat ini regulasi yang dipergunakan sebagai dasar hukum atas kasus-kasus cybercrime adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dengan adanya UU ITE ini diharapkan dapat melindungi masyarakat pengguna teknologi informasi di Indonesia, hal ini penting mengingat jumlah pengguna teknologi internet yang semakin meningkat dari tahun ke tahun. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, disisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan suatu perbuatan tindak pidana, kemajuan teknologi ini juga mempengaruhi gaya hidup dan pola pikir manusia faktanya saat ini banyak terjadi kejahatan dengan menggunakan teknologi informasi. Fenomena cybercrime yang berkembang dengan pesat yang tidak mengenal batas teritorial ini memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya.

Ironisnya, Indonesia pada saat ini menempati peringkat ke-2 (kedua) dunia dalam kasus kejahatan siber (cybercrime) setelah Ukraina.[10] Banyaknya kasus *Illegal Access* yang terjadi dalam kehidupan sehari-hari telah menunjukkan betapa pentingnya suatu pertanggungjawaban hukum dari pihak bank terhadap nasabah sebagai korban yang telah dirugikan akibat tindakan kejahatan *Illegal Access* serta tindakan kejahatan siber lainnya. Dapat kita lihat bersama juga bahwa suatu bentuk perlindungan hukum juga dibutuhkan oleh para nasabah yang menjadi korban tindakan kejahatan *Illegal Access*, karena dapat dipergunakan sebagai tameng hukum pada saat nasabah mengalami suatu kerugian akan

[9] Achmad Maulana Rezkian Noor, Faris Ali Sidqi, Sri Herlina, *SANKSI PIDANA TERHADAP PELAKU ILLEGAL ACCES DALAM SISTEM PERADILAN PIDANA INDONESIA,* e-Prints Uniska, https://eprints.uniska-bjm.ac.id/id/eprint/10645

[10]https://www.kominfo.go.id/index.php/content/detail/4698/Indonesia-Peringkat-ke-2-Dunia-susKejahatan-Siber/0/sorotan_media diakses pada Rabu, 20 November 2024 pukul 18.03 WIB.

E-ISSN : 2962-9713
P-ISSN : 2963-928X

sebuah tindakan kejahatan, juga dapat memudahkan pihak nasabah dalam mencari jalan keluar atau solusi dari suatu permasalahan hukum. Selain daripada itu, adanya upaya-upaya pencegahan yang juga merupakan sebuah bentuk perlindungan hukum,[11]sangatlah diperlukan guna meminimalisir atau mengurangi peluang terjadinya kasuskasus kejahatan di lingkup kegiatan perbankan seperti tindakan kejahatan skimming.

Menurut Peneliti pentingnya perlindungan hukum bagi korban kejahatan cyber, selain dalam kerangka mewujudkan negara hukum, hal ini penting dilakukan sebagai suatu tindakan preventif yang dilakukan oleh aparat penegak hukum dalam mengurangi ataupun mencegah terjadinya korban kejahatan dunia maya dan tentunya bukan hanya sebagai penampung laporan akan tetapi yang diharapkan adalah adanya tindakan nyata dari aparat penegak hukum sehingga masyarakat pengguna teknologi benarbenar merasa aman dalam melakaukan aktifitasnya di dunia maya.dan di rasa korban tindak pidana illegal access ini perlu mendapat kan perlindungan hukum yang jelas seperti Undang-undang informasi dan transaksi elektronik (UU ITE) atau yang disebut dengan cyberlaw, digunakan untuk mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya, baik transaksi maupun pemanfaatan informasinya. Pada UU ITE ini juga diatur berbagai macam hukuman bagi kejahatan melalui internet.

Dengan adanya undang-undang ITE diharapkan dapat memberikan rasa aman dan dapat melindungi bagi mereka yang menggunakan teknologi. Disamping itu, dalam keadaan tertentu dan membahayakan bagi mereka yang menjadi korban kejahatan teknologi juga berhak mendapatkan perlindungan hukum hal ini tercantum dalam Undang-undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban (UU PSK). Di dalam ketentuan Pasal 5 UU PSK.

Kemudian menurut Analisa dari peneliti korban juga berhak mendapatkan Hak-Hak sebagaimana dimaksud dalam ayat (1) diberikan kepada Saksi dan/atau Korban tindak pidana dalam kasus kasus tertentu sesuai dengan keputusan LPSK. Selanjutnya dalam ketentuan Pasal 1 ayat (2) UU PSK menyebutkan "korban adalah seseorang yang mengalami penderitaan fisik, mental dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana". Korban dalam hal ini adalah mereka yang telah dirugikan baik secara materi maupun non materi akibat dari kejahatan cybercrime. Dalam perlindungan hukum terhadap korban cybercrime secara mendasar ada dua model yaitu model hak-hak prosedural dan model pelayanan. [12]

Perlindungan hukum berhak didapatkan oleh korban dari kerjahatan teknologi dalam hal ini adalah kejahatan *illegal access* seperti tercantum dalam Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban (UU PSK). Perlindungan hukum terhadap nasabah bank sangat penting untuk menjaga kepercayaan masyarakat terhadap sistem perbankan. Tindak pidana ini melibatkan pelanggaran terhadap keamanan data nasabah, baik berupa pencurian informasi maupun pengubahan data secara tidak sah. Selain daripada Undang-Undang ITE dan Undang-Undang PDP, perlindungan terhadap korban kejahatan siber dalam hal ini *Illegal access* diatur juga melalui peraturan Otoritas Jasa Keuangan (OJK) No. 13/POJK.03/2022 tentang Perlindungan Konsumen di Sektor Jasa Keuangan.

. Tanggung jawab dalam kamus hukum diartikan sebagai suatu keharusan bagi seseorang untuk melaksanakan apa yang telah diwajibkan kepadanya. Dengan dasar hukum yang menyebutkan tentang perlindugan terhadap korban kejahatan siber dalam hal ini *illegal access*. Dapat dilakukan perlindungan secara pidana maupun secara perdata.

[11] Shidarta. 2006. Hukum Perlindungan Konsumen. (Jakarta: Grasindo). Cet 3. Hlm. 20
[12] Hermawan Bayu Aji Pratama, "Pelaksanaan Perlindungan Hukum Korban Tindak Pidana *Illegal Access*", Skripsi, Agustus 2020, hlm. 83-85

E-ISSN : 2962-9713
P-ISSN : 2963-928X

Pada perlindungan korban secara pidana, penuntutan sesuai dengan ketentuan UU ITE dan memberikan rasa aman kepada korban melalui mekanisme hukum yang ada. Dan pada perlindungan korban secara perdata berdasarkan suatu perbuatan melawan hukum telah diatur dengan jelas dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata. Adapun unsur-unsur pembuktian dari pasal 1365 ini, yaitu:

1. Perbuatan
2. Melawan Hukum
3. Adanya Kerugian
4. Adanya Hubungan Kausal antara Perbuatan dan Kerugian

Tujuan akhir dari sebuah pertanggungjawaban perbuatan melawan hukum ialah sebagai upaya untuk memulihkan suatu keadaan agar sekiranya dapat kembali seperti keadaan semula, seperti saat sebelum terjadi sengketa. Oleh sebab itu, dapat kita ketahui bersama bahwa berdasarkan ketentuan Pasal 1365 Kitab Undang-Undang Hukum Perdata, bentuk pertanggungjawaban dalam hukum perdata yaitu berupa sebuah ganti rugi.

Sehingga sudah sangat jelas bahwasanya dapat kita lihat bersama di dalam pengaturan kedua pasal Kitab Undang-Undang Hukum Perdata tersebut telah menyatakan secara tegas, bahwa pihak perbankan perlu untuk melakukan ganti rugi terhadap nasabah yang telah dirugikan akibat dari kesalahan ataupun kelalaian yang ditimbulkan oleh pihak perbankan itu sendiri,[13] maupun pihak lain sebagai pihak ketiga. Namun tidak menutup kemungkinan apabila tindak kejahatan tersebut diakibatkan oleh pihak ketiga atau pihak lain dan bukan pihak bank itu sendiri, maka pihak ketiga tersebutlah yang akan menerima sanksi pidana sebagaimana telah dipaparkan sebelumnya. Seperti halnya kerugian akibat kelalaian bank berupa tindakan kejahatan *illegal access,* maka pelaku tindakan kejahatan *illegal access* tersebut yang harus menerima sanksi berupa pidana penjara dan denda.

SIMPULAN

Teknologi telah menjadi semakin penting dalam kehidupan manusia, dan penggunaannya harus diprioritaskan untuk manfaatnya secara keseluruhan. Namun, penggunaan teknologi di sektor perbankan dapat menimbulkan risiko seperti pencurian data, manipulasi, dan akses ilegal. Penggunaan teknologi dalam perbankan tidak hanya bermanfaat bagi kehidupan manusia tetapi juga bagi sistem perbankan. Tindak pidana dalam perbankan merupakan masalah hukum yang mempengaruhi sektor perbankan dan kerangka hukum. Dewan Eropa - Konvensi Kejahatan Siber (ETS No. 185) menekankan perlunya undang-undang yang lebih ketat untuk mencegah manipulasi data ilegal. Teknologi informasi telah menjadi kontributor signifikan bagi kesejahteraan manusia dan tindakan hukum yang efektif. Namun, penggunaan internet untuk penyebaran informasi juga berbahaya, karena dapat menyebabkan akses informasi secara ilegal. Penggunaan manipulasi data ilegal dalam perbankan merupakan perhatian serius, karena dapat menyebabkan konsekuensi hukum bagi individu dan sektor perbankan. Oleh karena itu, sangat penting bagi bank untuk menerapkan undang-undang dan peraturan yang lebih ketat untuk melindungi data mereka dan mencegah akses dan manipulasi ilegal.

Sifat teknologi dan internet yang kompleks dan dinamis telah menyebabkan perkembangan kejahatan dunia maya, yang menjadi perhatian pemerintah yang semakin meningkat. Peraturan seperti Undang-Undang Informasi dan Transmisi Elektronik (ITE) 2008 bertujuan untuk melindungi masyarakat dari meningkatnya penggunaan teknologi internet. Tindakan ini juga membantu dalam mencegah akses ilegal dan bentuk kejahatan dunia maya lainnya. Indonesia telah terlibat dalam kasus kejahatan siber sejak Ukraina,

[13] Lihat Kitab Undang-Undang Hukum Perdata Pasal 1366.

E-ISSN : 2962-9713
P-ISSN : 2963-928X

dengan banyak kasus yang melibatkan akses ilegal. Undang-undang tersebut bertujuan untuk mencegah atau mengurangi konsekuensi dari akses ilegal, dan Undang-Undang ITE memberikan pedoman yang jelas untuk menggunakan internet untuk berbagai kegiatan. Undang-Undang ITE juga memberikan perlindungan bagi individu yang menggunakan teknologi, dan undang-undang tersebut didasarkan pada Undang-Undang LPSK, yang menyatakan bahwa "korban" mengacu pada individu yang memiliki konsekuensi fisik, mental, atau ekonomi akibat tindak pidana. Undang-Undang LPSK mendefinisikan "korban" sebagai individu yang telah dihukum secara salah oleh tindak pidana.

DAFTAR PUSTAKA

Buku:

Bala Tim PY. *Undang-Undang Informasi Dan Transaksi Elektronik: Seri Perundangundangan*. Yogyakarta: Pustaka Yustisia, 2019, hal. 33–34..

Soerjono Soekanto dan Sri Mamudi. *Penelitian Hukum Normatif*. Jakarta: CV. Rajawali, 1986, hal. 27.

Shidarta. *Hukum Perlindungan Konsumen*. Jakarta: Grasindo, 2006, Cet. 3, hlm. 20.

Peraturan Perundang-Undangan:

Seri Perjanjian Eropa 185 – Konvensi Tentang Tindak Pidana Telematika, Budapest, 23.IX.2001.

Kitab Undang-Undang Hukum Perdata Pasal 1365

Jurnal Ilmiah:

Muh. Alfian. "Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan." *Jurnal Kosmik Hukum* Vol. 17, No. 2 (Juni 2017), hlm. 150–151.

Galang Ramadhan Djokdja, dkk. "Pertanggungjawaban Pidana Pelaku Pembobolan Kartu Kredit Dalam Tindak Pidana Di Bidang Perbankan." *TATOHI Jurnal Ilmu Hukum* Vol. 2, No. 2 (2022), hal. 179.

Rezy Januar Wilyana, Imam Budi Santoso, dan Oci Senjaya. "Pembuktian Bukti Elektronik Di Persidangan." *Singaperbangsa Law Review* 1, no. 1 (2020): 164–183.

Achmad Maulana Rezkian Noor, Faris Ali Sidqi, dan Sri Herlina. "Sanksi Pidana Terhadap Pelaku Illegal Access Dalam Sistem Peradilan Pidana Indonesia." e-Prints Uniska. https://eprints.uniska-bjm.ac.id/id/eprint/10645.

Sumber Lainnya:

Deny Saputra. "Polri Ungkap Motif Pelaku 'Manipulasi' Data Nasabah BCA." *Kabar24*, Agustus 2023.

Hermawan Bayu Aji Pratama. "Pelaksanaan Perlindungan Hukum Korban Tindak Pidana Illegal Access." Skripsi, Agustus 2020, hlm. 83–85.

Kementerian Komunikasi dan Informatika. "Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber." Diakses melalui https://www.kominfo.go.id/index.php/content/detail/4698/Indonesia-Peringkat-ke-2-Dunia-sus-Kejahatan-Siber/0/sorotan_media pada Rabu, 20 November 2024, pukul 18.03 WIB.