Law, Development & Justice Review

Volume:	7	E-ISSN:	2655-1942
Number:	1	Terbitan:	April 2024
Page :	75-89		

Upaya Menghadapi Kejahatan Terhadap Sistem Keamanan Perbankan Indonesia di Era *Cyberspace*

Clara Mega Kharisma Sari,[1] Anita Zulfiani,[1] Suharto,[2] Muhyidin[2]

1. Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Sebelas Maret
E-mail: Clarakharisma7@student.uns.ac.id, Anitazulfiani@staff.uns.ac.id
2. Fakultas Hukum Universitas Diponegoro Semarang
E-mail: suharto@gmail.com, arfi27@gmail.com

Abstrak

Cyber Space merupakan media elektronik dalam jaringan komputer yang banyak dipakai dalam kehidupan saat ini, perkembangan dunia di Era *Cyber Space* berbanding lurus dengan kejahatan di bidang perbankan, Kejahatan tersebut diantaranya berkaitan dengan sistem keamanan perbankan, seperti; kejahatan carding, skimming, hacking, cracking, phising "*internet banking fraud*", malware "*virus/worm/trojan/bots*", *cybersquatting*, *money laundering, underground economy*. Tujuan penelitian untuk mengetahui dan menganalisis macam, macam, faktor penyebab dan kejahatan *Cyber Space* upaya penyelesaiannya. Manfaatnya, hasil penelitian dapat digunakan sebagai ide gagasan pemerintah dalam menghadapai kejahatan *Cyber Space* di masa sekarang. Penelitian ini menggunakan metode yuridis normatif yaitu pendekatan yang dilakukan berdasarkan bahan hukum utama dengan cara menelaah teori-teori, konsep-konsep, dan asas-asas yang berkaitan dengan sistem keamanan perbankan. Hasil penelitian menunjukkan bahwa upaya pencegahan terjadinya kejahatan sistem keamanan perbankan pemerintah dapat dilakukan melalui kebijakan sistem keamanan perbankan dan macam-macam narasi maupun sosialisasi system perbankan di masyarakat, serta penerapan prinsip-prinsip terkait dengan kemanan sistem perbankan. Orientasinya, pihak bank dapat memberikan pelayanan yang maksimal kepada nasabah serta memberikan manfaat yang berkelanjutan bagi berbagai pihak. Rekomendasi yang ditawarkan adalah mwujudkan sistem keamanan perbankan yang baik melalui usaha kerjasama antara pemerintah, pihak bank dan masyarakat dalam mewujudkan sistem keamanan yang mutakhir.

Kata Kunci: Kejahatan; Sistem; Keamanan; Perbankan

Absract

Cyber Space is an electronic media in computer networks that are widely used in today's life, the development of the world in the Cyber Space Era is directly proportional to crimes in the banking sector, these crimes are related to the banking security system, such as; carding crimes, skimming, hacking, cracking, phishing "internet banking fraud", malware "viruses/worms/trojans/bots", cybersquatting, money laundering, underground economy. The purpose of the study is to know and understand kinds, causative factors and crimes of Cyber Space efforts to solve them. The benefits, the results of the research can be used as an idea of government ideas in dealing with Cyber Space crime in the present. This research uses normative juridical method, which is an approach carried out based on main legal materials by examining theories, concepts, and principles related to the banking security system. The results showed that efforts to

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

prevent the occurrence of government banking security system crimes can be carried out through banking security system policies and various narratives and socialization of the banking system in the community, as well as the application of principles related to banking system security. Orientation, the bank can provide maximum service to customers and provide sustainable benefits for various parties. The recommendation offered is to realize a good banking security system through collaborative efforts between the government, the bank and the public in realizing a sophisticated security system.

Keyword: Crime; System; Security; Banking

A. Pendahuluan

Menurut Robert Kaiser, serangan siber terhadap Estonia pada tahun 2007 merupakan katalis bagi "terwujudnya perang *cyber*" sebagai objek kebijakan baru meskipun belum ada serangan yang dikatakan mencapai ambang batas serangan bersenjata dan memenuhi syarat sebagai tindakan kejahatan. perang yang terus mempengaruhi cara negara memandang ancaman perang cyber di masa depan.[1] Serangan-serangan ini terjadi seiring maraknya protes di kalangan minoritas Rusia terhadap keputusan pemindahan patung Prajurit Perunggu di Tallinn. Serangan DDOS3 ini melumpuhkan situs berbagai organisasi di negara ini, termasuk bank, media, kementerian, dan parlemen. Tahun berikutnya, pada bulan Juli 2008, gelombang serangan cyber terhadap situs web Georgia mendahului kedatangan tank Rusia di negara tersebut, serangan cyber pertama yang diketahui dikombinasikan dengan operasi militer darat. Meskipun sifatnya sederhana, dimensi umum dan spektakuler dari serangan-serangan ini memaksa negara-negara untuk menerima serangan-serangan tersebut. Sejak saat itu, serangan siber telah berlipat ganda dan, yang lebih penting, serangan tersebut menjadi lebih tepat sasaran, canggih, kreatif, dan merusak, sehingga menyebabkan negara-negara terus-menerus menyesuaikan diri terhadap ancaman yang terus berkembang, yang ditandai dengan serangkaian kejutan strategis dan perluasan ancaman yang terus-menerus.[2]

Tercatat sebanyak 741.441.648 ancaman *cyber* terjadi di Indonesia pada bulan Januari hingga Juli 2021. Ancaman siber ini mempunyai dampak yang sangat berbahaya bahkan dapat

[1] Kaiser. R, *Lahirnya Perang Cyber*, Geografi Politik, 46, 2015, hal.11–20.
[2] Frédérick Douzet & Aude Gery, *Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace*. Routledge: Journal of Cyber Policy. Vol.7, No.1, 2021, hal.7-8.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

mengancam pemilik akun yang terkena dampaknya.[3] Peristiwa yang terjadi baru-baru ini menunjukkan bahwa kejahatan meningkat di industri perbankan Indonesia, yang berdampak signifikan terhadap masyarakat internasional, perdagangan dan hubungan perburuhan. "Praktik bahaya moral dan ketidaktahuan akan prinsip-prinsip kehati-hatian" juga berkontribusi terhadap permasalahan ini.[4] Karena "kehidupan perbankan adalah jiwa kehidupan ekonomi", maka kejahatan di sektor perbankan tidak dapat dipisahkan dari kejahatan ekonomi[5] Conklin[6] menguraikan komponen-komponen kejahatan ekonomi, sebagai berikut :

1. Perbuatan melawan hukum yang mempunyai akibat pidana.
2. Perbuatan seseorang atau suatu korporasi dalam menjalankan tugas hukumnya atau dalam menjalankan usaha atau kegiatan komersialnya dalam bidang industri atau perdagangan.
3. Untuk: memperoleh uang atau kekayaan; menghindari membayar uang atau menghindari kehilangan kekayaan; memperoleh keuntungan komersial atau pribadi.

Perlindungan yang memadai terhadap korban kejahatan merupakan masalah baik di tingkat nasional maupun global. Hal ini memerlukan pertimbangan mendalam. Pembentukan Konvensi Internasional, "*Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power*" didasarkan pada Kongres PBB Ketujuh tentang Pencegahan Kejahatan dan Perlakuan terhadap Pelanggar, yang berlangsung di Milan, Italia pada bulan September 1985, menunjukkan pentingnya melindungi korban kejahatan.[7] Philip M. Hadjon mengatakan, perlindungan hukum adalah perlindungan kehormatan dan martabat, serta pengakuan hak asasi subjek hukum berdasarkan ketentuan hukum yang jauh dari kata sewenang-wenang. Perlindungan hukum juga mencakup seperangkat aturan yang dapat melindungi suatu hal dari hal lainnya. Artinya, dalam

[3] *Sahat Parulian, Devi Anassalifa Pratiwi* .et al, *Ancaman dan Solusi Serangan Siber di Indonesia*. Junal UPI: *Telecommunications, Networks, Electronics, and Computer Technologies* Vol.1 (2), 2021, hal.2-3.
[4] Muhamad Djumhana, *Hukum Perbankan di Indonesia*, Bandung: PT. Citra Aditya Bakti, 2021, hal.8-9.
[5] *Ibid.* hal.11.
[6] Muladi, & Barda Nawawi Arief, *Bunga Rampai Hukum Pidana*, Cetakan Pertama. Bandung: Alumni, 1992, hal. 63.
[7] Dikdik M. Arief Mansur dan Elisatris Gultom, *Urgensi Perlindungan Korban Kejahatan (Antara Norma Dan Realita*), Jakarta: PT. Raja Grafindo Persada, 2006, hal. 23-24.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

kaitannya dengan konsumen, hukum melindungi hak-hak konsumen dari segala pelanggaran terhadap hak-hak tersebut.[8]

Pada konteks ini, berbicara mengenai sistem keamanan perbankan maka perlindungan bagi konsumen dari ancaman kejahatan *cyber* merupakan salah satu isu krusial yang perlu dipecahkan. Maka dari itu untuk menyikapi kemajuan teknologi, sistem keamanan perbankan yang ada di Indonesia perlu diperbarui dan ditambahkan fitur keamanan baru. Hal ini dilakukan untuk mengantisipasi ancaman siber yang ada saat ini, menutup celah kerentanan dan meningkatkan tingkat keamanan, sehingga ketika entitas perbankan rajin melakukan update untuk perbaikan rutin, mengembangkan fitur atau meningkatkan keamanan sistem, harapannya bank sudah terbiasa menyelesaikannya. tanpa mengorbankan layanan yang ditawarkannya kepada kliennya.

Oleh karena itu, sangat penting diperhatikan pertimbangan-pertimbangan dalam melakukan pembaruan aplikasi, seperti; memastikan ketersediaan layanan, menjaga stabilitas sistem elektronik, dan meningkatkan keamanan sistem terhadap berbagai ancaman siber. Dengan demikian kerjasama antara pemerintah, pihak Bank, dan masyarakat sangat diperlukan demi terwujudnya suatu sistem kemanan perbankan yang baik dan mutakhir.

Berdasarkan uraian latar belakang di atas, maka sangat penting diadakan penelitian tentang bagaimanakah upaya pemerintah menghadapi kejahatan terhadap sistem keamanan perbankan Indonesia di era *cyberspace.* Tujuan penelitian untuk mengetahui dan menganalisis macam, macam, faktor penyebab kejahatan *Cyber Space* dan upaya penyelesaiannya. Manfaat penelitian dapat digunakan sebagai ide gagasan pemerintah dalam menghadapai kejahatan *Cyber Space* di masa sekarang.

B. Metode Penelitian

Jenis penelitian ini adalah library research dengan menggunakan pendekatan yuridis normatif, yaitu pendekatan berbasis hukum yang mengkaji teori, konsep, dan asas terkait penerapan undang-undang terkait dengan sistem keamanan perbankan di Indonesia. Penelitian ini menggunakan

[8] Mochammad Najib Imanullah Zennia Almaida, *Perlindungan Hukum Preventif Dan Represif Bagi Pengguna Uang Elektronik Dalam Melakukan Transaksi Tol Nontunai*, Jurnal Private Law, Vol. 9, No. 1, 2021, hal. 222.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

pendekatan kasus yang mengkaji kasus-kasus yang berkaitan dengan topik tersebut, serta pendekatan hukum yang mengkaji peraturan perundang-undangan yang berkaitan dengan topik tersebut. Kebaharuan dalam penulisan ini terletak pada instrumen yang digunakan dalam objek penelitian di mana dalam penelitian ini membahas bukan hanyak faktor pemerintah yang dapat mempengaruhi terkait sistem kemanan perbankan akan tetapi di dalam penelitian ini di bahas lebih mendalam dengan memasukkan faktor pihak bank serta komponen masyarakat untuk melakukan upaya terbaik supaya terwujudnya suatu sistem kemanan perbankan yang baik di Indonesia.

C. Hasil Penelitian dan Pembahasan

Kejahatan dunia maya masih relatif tinggi. Serangan hacker terhadap keamanan perbankan online terus mengintai setiap saat. Bank of America juga menghabiskan lebih dari $1 miliar per tahun untuk keamanan siber. Keamanan cyber sendiri merupakan seperangkat alat, kebijakan keamanan, perlindungan keamanan, tindakan, pelatihan, jaminan, dan teknologi yang digunakan untuk melindungi lingkungan internal lingkungan siber aktif dan organisasi pengguna. Organisasi ini terintegrasi dengan menghubungkan komputasi, infrastruktur, aplikasi, sistem komunikasi dan semua informasi yang dikirim melalui lingkungan virtual.[9] Kejahatan yang dikenal sebagai "kejahatan kerah putih" juga dikenal sebagai "kejahatan Profesional" telah meningkat di kalangan profesional karena mereka memiliki akses yang lebih besar terhadap sistem.[10] Oleh karena itu,menyatakan bahwa melindungi karyawan ini dari sistem informasi menjadi lebih sulit dan rumit karena mereka berasal dari dalam organisasi.[11]

Karena informasi adalah aset berharga dan rahasia, maka pihak Bank harus mencegah orang lain mengaksesnya. Oleh sebab itu Bank sangat memperhatikan keamanan informasi. Maka

[9] H. Ardiyanti, *Cyber-security dan Tantangan Pengembangannya di Indonesia*. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional,Vol. 10, No.1. 2016, hal.7.

[10] Loch, Karen D., Houston H. Carr dan Merrill E. Warkentin, *Ancaman Terhadap Sistem Informasi: Realitas Hari Ini, Pemahaman Kemarin. MIS Triwulanan,* 1992*, hal.*173 - 186.

[11] Whitman, SAYA *dalam Membela Dunia: Memahami Ancaman Terhadap Keamanan Informasi*. Jurnal Internasional Manajemen Informasi*,* Vol. 24, No. 1, 2004, hal.43-57.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

terhadap pengendalian keamanan yang memadai harus terus ditinjau untuk mencegah aset dari digunakan, diungkapkan, diubah, atau dihancurkan secara tidak disengaja.[12] Pada hakekatnya sistem keamanan merupakan garda terdepan dalam sistem perbankan, karena tanpa sistem keamanan maka suatu perbankan tidak dapat berjalan sebagaimana mestinya. Konsumen akan memberikan kepercayaannya kepada pihak Bank salah satunya dengan menilai apakah sistem keamanan yang dimiliki Bank tersebut mutakhir, apabila konsumen menilai bahwa sistem kemanan Bank tersebut lemah maka konsumen tidak akan tertarik untuk menaruh dana simpanan maupun suatu yang berharga pada Bank tersebut.

Cybersecurity mencakup memastikan pencapaian dan pemeliharaan karakteristik keamanan organisasi dan aset pengguna terhadap potensi ancaman keamanan. Tujuan umum dari *cybersecurity* adalah menjaga integritas, yang memungkinkan upaya mengurangi terjadinya ancaman *cyber* yang serius. Lima bidang kerja yang membentuk *cybersecurity* secara global:[13]

1. Kepastian hukum (legalitas cybercrime)
2. Teknis dan tindakan procedural
3. Struktur organisasi
4. Peningkatan kapasitas dan pendidikan pengguna
5. Kerjasama internasional.

Karena kenyataan bahwa tingkat kejahatan dunia maya di Indonesia sudah mencapai tingkat yang memprihatinkan, Indonesia saat ini berada dalam keadaan mendesak untuk melindungi keamanan dunia maya atau *cybersecurity*. Data yang dikumpulkan oleh CIA menunjukkan bahwa kerugian yang disebabkan oleh tindak kejahatan dengan memanfaatkan dan tindak kejahatan di dunia cyber di Indonesia telah mencapai 1,20% dari total kerugian yang disebabkan oleh cybercrime secara global. Hal ini menunjukkan bahwa cybercrime di Indonesia sudah

[12] Zaini Zainol, Sherliza Puat Nelson, et al, *Internal Human Based Threats and Security Controls in Computerized Banking Systems: Evidence from Malaysia*. Sciverse ScientDirect. Procedia - Social and Behavioral Sciences 65, 2012, hal.199 – 204.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

mengkhawatirkan.[14] Pada hasil penelitian ini akan Karena sifat uergensinya terkait dengan sistem keamanan perbankan ini hal tersebut akan lebih lanjut dibahas dalam pembahasan sebagai berikut:

1. Kejahatan terhadap sistem Keamanan Perbankan Indonesia di Era *Cyberspace*

Cybersecurity adalah kegiatan untuk melindungi sistem komputer, seperti program aplikasi, data, dan informasi yang ada, dari berbagai serangan dan akses yang tidak sah. Tindakan keamanan siber ini termasuk alat, aturan, gagasan keamanan, dan lainnya yang dapat digunakan untuk melindungi aset perusahaan dan pengguna. Untuk menerapkan keamanan cyber di perusahaan atau yayasan Anda, diperlukan anggaran besar dan laporan keuangan yang tepat.[15] Kejahatan siber adalah jenis kejahatan yang berkaitan dengan penggunaan teknologi informasi yang tidak terkendali dan ditandai dengan metode teknologi yang mengandalkan tingkat keamanan dan keandalan yang tinggi dari data yang dikirimkan dan diakses oleh pengguna internet.[16] Kejahatan dunia maya hadir dalam berbagai bentuk dan selalu berubah. Penjahat dunia maya menggunakan sarana elektronik seperti *skimming, malware*, dan peretasan saat melakukan transaksi di sektor perbankan, [17] Ada beberapa faktor yang mempengaruhi terjadinya suatu kejatahan sistem keamanan perbankan, diantaranya:

a. Faktor Dari Pemerintah

Berbicara mengenai kejahatan dalam sistem keamanan perbankan hal tersebut tentunya tidak terlepas dari peran pemerintah sebagai pengelola suatu negara, pemerintah juga memberikan konstribusi terkait dengan sistem keamanan perbankann baik konstribusi tersebut bisa dalam bentuk kebijakan maupun program-program yang dimiliki pemrintah Indonesia. Hukum pidana dan perdata dapat diterapkan untuk melindungi nasabah bank yang menjadi korban kejahatan

[14] Handrini Ardiyanti, 2014, *Cyber Security Dan Tantangan Pengembangannya. Pengolahan Data dan Informasi Sekretariat Jenderal DPR RI*: Politicia. Vol.X No.1.

[15] Marcelina, D., Suryati, & Yulianti, E, *Workshop Teknologi Informasi "Dasar Cyber Security" Pada SMK PGRI Tanjung Raja Ogan Ilir (OI)*, Jurnal Abdimas Mandiri. Vol. 7, No. 2, 2022, hal. 67-72.

[16] Suharto, M. A., & Apriyani, M. N., *Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional,* Jurnal Risalah Hukum, Vol. 12, No.2, 2021, hal.98-107.

[17] Faridi, M. K, *Kejahatan Siber dalam Bidang Perbankan. Cyber Security dan Forensik Digital*, Vol. 1, No.2, 2018, hal.57–61.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

cyber. Apabila nasabah mengalami kerugian finansial akibat kejahatan bank yang bukan disebabkan oleh nasabah itu sendiri, maka pelaku usaha yaitu bank bertanggung jawab untuk mengganti kerugian yang diderita nasabah sebagai konsumen. OJK juga bertanggung jawab jika nasabah kehilangan uang dalam transaksi perbankan.

Pemerintah dalam konteks pemangku jabatan negara memiliki peran berkaitan dengan kebijakan terkait dengan sistem kemanan perbankan. Masih banyak terjadinya kejahatan terhadap sistem keamanan perbankan salah satu faktor yang menyebabkan adalah pertama, lemah nya regulasi yang ada saat ini sehingga masih terjadi banyak kejahatan sistem kemanan perbankan. Pemerintah Indonesia harus lebih berhati-hati dalam menyikapi kemajuan teknologi informasi dan masyarakat dalam pembuatan dan penerapan peraturan perundang-undangan. Dengan demikian, perlindungan terhadap permasalahan yang berkaitan dengan kemajuan saat ini, khususnya teknologi terkait dengan sistem keamanan perbankan, menjadi lebih efektif, tepat waktu dan tepat sasaran. Kedua, sering berubah-ubahnya regulasi juga menjadi salah satu faktor terjadinya kejahatan terhadap sistem keamanan perbankan. Pemerintah dapat mendorong sektor swasta dan masyarakat menuju praktik keamanan yang lebih baik dengan menetapkan peraturan dan kebijakan yang tepat.

Ketiga, di Indonesia sendiri tim reaksi cepat untuk menindaklanjuti serangan-serangan siber yang terjadi masih belum efektif hal ini terhalang oleh berbagai kendala seperti kendala prosedur yang rumit atau kendala dari aparat penegak hukumnya itu sendiri dalam hal ini artinya aparat penegak hukum kurang professional dalam menghadapi permasalahan tersebut. Aparat penegak hukum di nilai lambat dalam menangai perkara *cyber* hal ini disebabkan alat untuk mendetekti atau mencegat kejahatan cyber tersebut masih belum mutakhir dengan perkembangan kejahatan cyber saat ini. Untuk program seperti inisiatif dan program yang akan memberdayakan masyarakat untuk mengatasi ancaman dunia maya yang seharusnya dilakukan pemerintah masih kurang sehingga masyarakat masih banyak yang belum aware terkait dengan keamanan rekening nya.

Keempat, Pemerintah juga bertindak dengan menyediakan sumber daya dan pelatihan bagi masyarakat dan profesional IT untuk membangun kemampuan keamanan siber. Dalam prakteknya program pelatihan yang ada selama ini masih kurang dalam hal ini seharusnya pemerintah dapat

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

melakukan kerjasama dengan pihak Bank terkait dengan program pelatihan tersebut demi terwujudwan lingkungan Indonesia yang aman dari kejahatan cyber.

b. Faktor dari Pihak Bank

Kejahatan terhadap sistem keamanan perbankan apabila ditinjau dari pihak perbankan sendiri faktor yang dapat menyebabkan terjadinya kejahatan sistem kemanan perbankan adalah yang pertama, kegagalan sistem. Kegagalan sistem ini dapat disebabkan karena adanya kerusakan sistem (misalnya turunnya jaringan atau server down), dan dalam skala luas bisa disebabkan karena bencana alam. Artinya pihak bank dalam hal ini apabila terjadi suatu peristiwa yang menyebabkan kekacauan dalam sistem keamanannya masih dianggap kurang sigap dan untuk menghadapi peristiwa tersebut Bank di Indonesia saat ini seharusnya memiliki sistem keamanan ganda jadi apabila sistem pertama terjadi kelumpuham maka dapat digunakan sistem kedua begitu juga seterusnya.

Kedua, Di sektor perbankan, terdapat beberapa kelalaian yang disengaja, hal tersebut dilakukan dengan menggunakan teknik seperti membuat atau menyebabkan pencatatan palsu dalam proses akuntansi atau pelaporan, atau dalam dokumen atau laporan yang berkaitan dengan kegiatan usaha, laporan transaksi atau rekening bank. Menghilangkan atau tidak mencatat dalam akuntansi atau laporan, serta dalam dokumen atau laporan kegiatan komersial, transaksi atau rekening bank. Mengubah, mengaburkan, menyembunyikan, menghapus atau menghilangkan keberadaan suatu entri dalam akuntansi atau pelaporan, serta dalam dokumen atau laporan bisnis, laporan transaksi atau rekening bank, atau dengan sengaja mengubah, mengaburkan, menghilangkan, menyembunyikan atau menghancurkan catatan tersebut akuntansi tentu hal tersebut juga dapat membuat peluang pembobolan rekening nasabah di mana apabila yang di input data tidak sesuai dengan akta asli maka akan menjadi sulilt apabila dilakukan penelusuran terkait permasalahan yang terjadi. Hal semacam itu dapat disebabkan karena SDM yang rendah.

Ketiga, Kurang memadai fasilitas yang ada di masyarakat. ATM harus ditempatnya di wilayah yang strategis dengan kelengkapan cctv serta dilakukan operasi secara berkala. Pada kenyataannya banyak sekali ATM di Indonesia yang sering troble dan ATM terlihat kumuh serta jarang dilakukan operasi di beberapa titik ATM hal ini tentu dapat memicu terjadinya suatu tindak

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

pidana kejahatan cyber seperti kejahatan card skimming. Ketersediaan Infrastruktur dan Kapasitas Teknologi yang rendah ini dapat menjadi celah besar bagi pelaku tindak kejahatan.oleh sebab itu sistem keamanan perbankan Indonesia harus selalu mutakhir dengan memasukkan fitur-fitur keamanan baru yang sesuai dengan kemajuan teknologi.

c. Faktor dari Masyarakat

Kejahatan terhadap sistem keamanan perbankan juga dapat ditinjau dari pidak masyarakat, di mana masyarakat disini posisinya adalah sebagai nasabah Bank. Faktor penyebab munculnya kejahatan cyber dalam sistem keamanan perbankan diantaranya seperti ancaman serangan phising hal ini dapat terjadi karena minimnya pengetahuan pengguna, psikologis, dan privasi social networking services pengguna. Berdasarkan hal tersebut dapat ditarik kesimpulan bahwa faktor apa yang dapat menyebabkan terjadinya kejahatan cyber adalah sebagai berikut: pertama, komponen utamanya adalah Tingkat kesadaran masyarakat terhadap haknya menjadi kelemahan nasabah. Hal tersebut dapat menempatkan nasabah pada posisi yang lemah, seperti yang sering terjadi saat ini di kalangan masyarakat yang mengeluh baik terhadap sistem maupun bank, seperti pengurangan rekening nasabah tanpa Data rahasia klien telah diretas tanpa sepengetahuan mereka. Pengiriman uang yang dilakukan melalui online banking tidak masuk ke rekening tujuan oleh pihak yang tidak bertanggung jawab. Dan masyarakat secara umum harus sadar bagaimana melindungi diri dari data pribadinya di Internet untuk mencegah kejahatan terkait penyalahgunaan data pribadi.

Kedua, faktor psikologis di dalam aspek pengambilan suatu keputusan untuk melakukan transaksi hal ini sangat dipengaruhi oleh beberapa faktor, salah satunya adalah faktor psikologis seseorang dan pemahaman akan informasi yang didapatkan. Dalam hal ini psikologis masyarakat dapat dimainkan oleh pelaku kejahatan di mana pelaku dapat memberikan berbagai upaya penawaran yang menarik sehingga masyarakat tergiur akan penawaran yang diberikan. Ketiga, faktor budaya di mana budaya yang ada di masyarakat dapat memepengaruhi gaya hidup, cara hidup masyarakat di lingkungannya, missal; karena dilingkungan yang hedon maka secara tidak langsung ada keinginan seseorang untuk menyesuaikan dengan lingkungan tersebut. Karena keinginannya tersebut masyarakat melakukan berbagai cara supaya keinginannya terpenuhi salah

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

satu nya apabila pelaku kejahatan cyber membagikan pesan dengan menyertakan link di mana dalam pesan tersebut berisi bahwa penerima pesan mendapatkan hadiah misal dari Bank A, kemudian karena faktor budaya dan cara pandang yang salah tadi dapat menyebabkan seseorang meng klik link tersebut yang padahal dampaknya adalah terkurasnya rekening di bank.

Keempat, faktor pendidikan ini merupakan faktor yang tidak kalah penting dengan faktor sebelumnya, dikarenakan pendidikan seseorang dapat mempengaruhi cara berfikir dan cara pandang seseorang terhadap suatu hal. Misal apabila seseorang telah mendapat ilmu yang berkaitan dengan bagaimana menjaga keamanan rekeningnya dari tindak kejahatan maka orang tersebut akan menerapkan ilmu yang di dapatkannya tersebut sehingga kejahatan dalam perbankan dapat terhindarkan.

2. Upaya Pemerintah, Perbankan, Masyarakat dalam Menghadapai Kejahatan Sistem Kemanan Bank di Era *Cyberspace*

Perkembangan teknologi informasi di sektor perbankan berpotensi menimbulkan risiko *cybercrime* yang dapat merugikan nasabah, namun juga dapat membantu industri perbankan dan nasabah. finansial Sebagai layanan keuangan yang berbasis pada kepercayaan masyarakat, industri perbankan harus terus meningkatkan keamanannya dalam hal keamanan siber untuk selalu menjaga kepercayaan masyarakat. Bentuk pertahanan UUPK, UU Perbankan, UU Telekomunikasi, dan UU Jasa Keuangan telah mengatur undang-undang pelanggan tentang kejahatan siber. Peraturan Otoritas Jasa Keuangan juga mengaturnya secara teknis. cepat, perjanjian saat ini Hal ini menciptakan kewajiban bank untuk terus melindungi nasabah dari kejahatan dunia maya global. Langkah-langkah yang dapat dilakukan jika nasabah mengalami kerugian finansial akibat kejahatan siber adalah diselesaikan melalui jalur non-litigasi dan litigasi. Hasil penelitian menunjukkan bahwa, penyelesaian masalah kerugian nasabah lebih banyak dilakukan melalui non litigasi, yakni musyawarah dan mediasi, karena proses peradilan menimbulkan kerugian bagi konsumen sebab rumitnya penyelidikan dan pengungkapan kejahatan dunia maya[18]

[18] Kukuh Dwi Kurniawan,Dwi Ratna Indri Hapsari, *Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia : Ananlisa Perlindungan Hukum Bagi Nasabah*. Pleno Jure: Jurnal Ilu Hukum.Vol 10, No, 2, 2021, hal. 23.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

Beberapa cara untuk meningkatkan keamanan sistem informasi termasuk meningkatkan pengetahuan SDM terkait ancaman siber, menerapkan sertifikasi kesiapan, dan mengadopsi domain keamanan dari negara lain. Selain itu, pemetaan jenis serangan siber dan pemilihan teknologi keamanan yang sesuai juga penting. Beberapa upaya lain termasuk pembaruan sistem operasi secara berkala, menerapkan enkripsi pada data, mengontrol akses, menggunakan teknologi firewall, serta mengimplementasikan prosedur operasional standar (SOP) dan kebijakan privasi. Penelitian ini dapat menjadi panduan dalam mengembangkan kebijakan dan langkah-langkah yang efektif dalam mempertahankan keamanan sistem informasi.

Kita membutuhkan sejumlah besar organisasi profesional yang mampu menghadapi bahaya keamanan siber, bahkan pada tingkat paling mutakhir sekalipun, keamanan siber harus diintegrasikan ke dalam program, bersama dengan proses, infrastruktur, dan teknologi. Pemerintah diharapkan untuk fokus pada keamanan siber untuk mengatasi masalah privasi data.[19] Pemerintah dapat melakukan berbagai upaya, termasuk tindakan non-Pidana dan Pidana, sehubungan dengan semua permasalahan tersebut di atas. Upaya non-kriminal dalam memberantas tindak pidana yang berkaitan dengan teknologi informasi, baik preventif maupun preventif, penangkalan atau pengendalian sebelum terjadinya tindak pidana, harus dilakukan dengan kemampuan dan kemauan sesuai dengan hal-hal sebagai berikut:[20]

1. Menemukan dan melacak penjahat secara online memerlukan kolaborasi internasional oleh karena itu kerjasama internasional dalam rangka pemberantasan kejahatan cyber sangat diperlukan.
2. Untuk memerangi kejahatan dunia maya di berbagai negara, penting bagi setiap negara untuk berkomunikasi, menyepakati, dan berkolaborasi mengenai yurisdiksi dan kebijakan non-kriminal (di luar hukum pidana).

[19] Nihal Jayawickrana, *The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence*. United Kingdom: Cambridge University Press, 2002, hal. 45.
[20] Dwikari Nuristiningsih, *Upaya Penal Dan Non Penal Dalam Menanggulangi Tindak Pidana Teknologi Informasi*, Vol.XXIII, No.2, 2023, hal.88.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

3. Harus ada pernyataan bahwa pemerintah dan industri akan bekerja sama untuk mencegah dan mengendalikan kejahatan dunia maya.
4. Internet adalah lokasi yang aman untuk memanfaatkan inovasi teknologi.
5. Memberikan pemahaman kepada masyarakat di era teknologi informasi.
6. Pemanfaatan komputer untuk keamanan siber, seperti memperbanyak berita edukasi melalui media massa dan elektronik, serta melakukan kegiatan sosialisasi dan diseminasi yang dilakukan oleh pihak berwenang.

D. Kesimpulan

Kejahatan cyber adalah jenis kejahatan yang berkaitan dengan penggunaan teknologi informasi yang tidak terkendali dan ditandai dengan metode teknologi yang mengandalkan tingkat keamanan dan keandalan yang tinggi dari data yang dikirimkan dan diakses oleh pengguna internet. Di era sekarang, telah muncul kejahatan cyber di bidang perbankan yang berkaitan dengan sistem keamanan perbankan, penyebabnya berasal dari faktor pemerintah, pihat swasta (Bank), dan pihak masyarakat. Faktor dari pemerintah meliputi; lemahnya regulasi yang ada saat ini sehingga masih terjadi banyak kejahatan sistem kemanan perbankan; seringnya terjadi perubahan regulasi yang ditetapkan pemerintah; tim reaksi cepat yang menindaklanjuti serangan-serangan siber yang terjadi masih belum efektif; dan kurangnya peran Pemerintah dalam bertindak dengan menyediakan sumber daya dan pelatihan bagi masyarakat dan profesional IT untuk membangun kemampuan keamanan siber. Faktor dari swasta, meliputi; kegagalan sistem; terdapat beberapa kelalaian yang disengaja dari pihak perbankan; kurangnya fasilitas pelayanan untuk masyarakat. Faktor masyarakat adalah kurangnya tingkat kesadaran masyarakat terhadap keamanan rekening pribadi.

Upaya untuk mencegah terjadinya kejahatan cybercrime antara lain; meningkatkan kesadaran masyarakat untuk mengamankan siber; memberikan edukasi masyarakat tentang praktik keamanan yang baik dan aman di dunia maya; menciptakan lingkungan yang mendukung keamanan siber. Pemerintah juga mempunyai tanggung jawab untuk menyediakan sumber daya dan pelatihan bagi masyarakat umum dan profesional IT untuk mengembangkan keterampilan

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

keamanan siber. Keberhasilan dalam menghadapi ancaman siber yang semakin meningkat bergantung pada kolaborasi antara pemerintah dan sektor swasta, yakni perbankan. Dan untuk masyarakat diharapkan menerapkan prinsip kehati-hatian dan saling mengingatkan satu sama lain terkait dengan kejahatan Cyber supaya terhindar dari dampak yang timbul dari kejahatan tersebut.

Daftar Pustaka

Buku

Dikdik M. Arief Mansur dan Elisatris Gultom, 2006, *Urgensi Perlindungan Korban Kejahatan (Antara Norma Dan Realita).* Jakarta: PT. Raja Grafindo Persada.

Jayawickrana. Nihal, 2002, *The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence*. United Kingdom: Cambridge University Press.

Muladi, & Barda Nawawi Arief, 1992, *Bunga Rampai Hukum Pidana*, Cetakan Pertama. Bandung: Alumni.

Muhamad Djumhana, 2021, *Hukum Perbankan di Indonesia*. Bandung: PT. Citra Aditya Bakti.

Jurnal

Ardiyanti. H, 2016, *Cyber-security dan tantangan pengembangannya di indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*,Vol.X.No.1.

Dwikari Nuristiningsih, 2023, *Upaya Penal Dan Non Penal Dalam Menanggulangi Tindak Pidana Teknologi Informasi,* Vol.XXIII, No.2.

Faridi, M. K, 2018, *Kejahatan Siber dalam Bidang Perbanka*n. Cyber Security Dan Forensik Digital, Vol.I. No.2.

Frédérick Douzet & Aude Gery, 2021, *Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace*. Routledge: Journal of Cyber Policy. Vol.VI. No.1. Juni.

Volume: 7 E-ISSN: 2655-1942
Number: 1 Terbitan: April 2024
Page : 75-89

Handrini Ardiyanti, 2014, *Cyber Security Dan Tantangan Pengembangannya. Pengolahan Data dan Informasi Sekretariat Jenderal DPR RI*: Politicia. Vol.X No.1.

Kaiser. R, 2015, "*Lahirnya Perang Cyber*." Geografi Politik, hlm.46.

Kukuh Dwi Kurniawan,Dwi Ratna Indri Hapsari, 2021, *Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia : Ananlisa Perlindungan Hukum Bagi Nasabah*. Pleno Jure: Jurnal Ilu Hukum.Vol 10, No, 2.

Loch, Karen D., Houston H. Carr dan Merrill E. Warkentin, 1992, *Ancaman terhadap sistem informasi: Realitas hari ini, pemahaman kemarin*. *MIS Triwulanan.*

Marcelina, D., Suryati, & Yulianti, E, 2022, Workshop *Teknologi Informasi "Dasar Cyber Security" Pada SMK PGRI Tanjung Raja Ogan Ilir (OI)*. Jurnal Abdimas Mandiri. Vol.VI.No. 2.

Mochammad Najib Imanullah Zennia Almaida, 2021, *"Perlindungan Hukum Preventif Dan Represif Bagi Pengguna Uang Elektronik Dalam Melakukan Transaksi Tol Nontunai*," Private Law 9, no. 1 : 222.

Muladi, & Barda Nawawi Arief, 1992, *Bunga Rampai Hukum Pidana*, Cetakan Pertama. Bandung: Alumni.

Sahat Parulian, Devi Anassalifa Pratiwi .et al. 2021, *Ancaman dan Solusi Serangan Siber di Indonesia.* Junal UPI: Telecommunications, Networks, Electronics, and Computer Technologies Vol.1 (2).

Suharto, M. A., & Apriyani, M. N, 2021, *Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. Jurnal RisalahHukum, Vol.XVII, No.2*, hlm.98-107.

Whitman. SAYA, 2004, *Dalam membela dunia: memahami ancaman terhadap keamanan informasi. Jurnal Internasional Manajemen Informasi,* 24 (1).

Zaini Zainol, Sherliza Puat Nelson, et al, 2012, *Internal Human Based Threats and Security Controls in Computerized Banking Systems: Evidence from Malaysia*. Sciverse ScientDirect. Procedia - Social and Behavioral Sciences, hlm.65.