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

**Clara Mega Kharisma Sari1, Anita Zulfiani2,**

Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Sebelas Maret

[Clarakharisma7@gmail.com](mailto:Clarakharisma7@gmail.com)

***Absract***

*In this Cyberspace Era, the system of life in society, both Indonesian and world, has changed a lot, this can have a complete impact on people's lives, both in the form of positive and negative impacts. Along with the development of the cyber world, this is directly proportional to crime in the banking sector, these crimes are related to the banking security system. There are many crimes against the banking security system including carding crimes "credit card fraud", ATM or EDC "skimming", hacking, cracking, phishing "internet banking fraud", malware "virus/worm/trojan/bots", cybersquatting, pornography, gambling online, transnational crime “drug trafficking, mafia, terrorism, money laundering, human trafficking, underground economy”. From these various crimes, to prevent crimes against the banking security system, the government can carry out various efforts, including efforts related to banking security system policies and various efforts that can be made, such as various narratives and outreach to the public. Apart from the government, banks and the public must also implement principles related to banking system security. This research uses a normative juridical method, namely an approach based on the main legal material by examining theories, concepts and principles related to the banking security system. In order to achieve a good banking security system, cooperation between the government, the bank and the community is required.*

***Keyword : Crime ; System ; Security ; Banking.***

**Abstrak**

Dalam Era *CyberSpace* ini telah banyak merubah sistem kehidupan dalam masyarakat baik masyarakat Indonesia maupun dunia, hal tersebut sepenuhnya dapat membawa dampak bagi kehidupan masyarakat baik berupa dampak positif maupun dampak negatif. Seiring dengan perkembangan dunia *cyber* maka berbanding lurus dengan kejahatan di bidang perbankan, Kejahatan tersebut diantaranya bekaitan dengan sistem keamanan perbankan. Banyak sekali kejahatan terhadap sistem keamanan perbankan diantara nya kejahatan carding “*credit card fraud”*, ATM atau EDC “skimming”, hacking, cracking, phising “i*nternet banking fraud*”, malware “*virus/worm/trojan/bots*”, cybersquatting, pornografi, perjudian online, transnasional crime “perdagangan narkoba, mafia, terorisme, *money laundering, human trafficking, underground economy*”. Dari berbagai kejahatan tersebut untuk mencegah terjadinya kejahatan terhadap sistem keamanan perbankan pemerintah dapat melakukan berbagai upaya diantaranya upaya yang berkaitan dengan kebijakan sistem keamanan perbankan dan bebagai upaya yang dapat dilakukan seperti macam-macam narasi maupun sosialisasi terhadap masyarakat. Selain pemerintah, pihak perbankaan dan pihak masyarakat juga harus menerapkan prinsip-prinsip terkait dengan kemanan sistem perbankan. 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. Demi tercapainya suatu sistem keamanan Perbankan yang baik perlu adanya kerjasama antara pemerintah, pihak Bank dan masyarakat.

**Kata Kunci : Kejahatan ; Sistem ; Keamanan ; Perbankan.**

### 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]](#footnote-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]](#footnote-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 mengancam pemilik akun yang terkena dampaknya.[[3]](#footnote-3) Ancaman *cyber* terhadap sistem kemanan perbankan merupakan salah satu isu krusial yang sangat perlu diperhatikan, selain berkaitan dengan dana nasabah yang ada di rekening Bank, data pribadi nasabah yang ada direkening Bank juga merupakan suatu hal yang sangat penting untuk dijaga kerahasiannya karena apabila data tersebut disalah gunakan maka hal tersebut dapat menyebabkan terjadinya suatu kerugian bagi nasabah baik itu kerugian yang bersifat materil maupun bukan. Salah satu hak asasi manusia yang menjadi bagian dari perlindungan diri pribadi adalah perlindungan data pribadi. Pasal 28G UUD 1945 memuat perlindungan diri ini. Perlindungan atau privasi pribadi ini bersifat universal dan diakui oleh banyak negara. Peraturan Umum Perlindungan Data telah berlaku di 28 negara anggota Uni Eropa (UE) sejak Mei 2018. Jumlah ini terus meningkat sebagai respons terhadap pentingnya perlindungan data warganya.

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]](#footnote-4) Karena “kehidupan perbankan adalah jiwa kehidupan ekonomi”, maka kejahatan di sektor perbankan tidak dapat dipisahkan dari kejahatan ekonomi.[[5]](#footnote-5)

Berikut ini Conklin menguraikan komponen-komponen kejahatan ekonomi:[[6]](#footnote-6)

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.

Kejahatan perbankan berdampak pada simpanan nasabah pada bank sehingga berdampak pada kepentingan berbagai pihak, antara lain bank sebagai badan usaha, nasabah, sistem perbankan, otoritas perbankan, pemerintah, dan masyarakat pada umumnya. Ronny Prasetya mengatakan kejahatan dunia maya menimbulkan banyak masalah baru dan serius secara global dan sulit untuk memastikan bahwa hukum mampu mengendalikannya. Permasalahan kedua yang paling mengkhawatirkan dalam dunia perbankan adalah kejahatan ekonomi, seperti pencurian kartu ATM dan uang, terutama yang dilakukan di Asia.[[7]](#footnote-7)

Berdasarkan uraian di atas maka dapat disimpulkan bahwa pentingya sistem keamanan perbankan. Di dalam penulisan tulisan ini penulis menggunakan pendekatan hukum 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 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 dimana dalam penelitian ini mebahas 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.

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 Crimeand Abuse of Power” Deklarasi Prinsip-prinsip Dasar Keadilan bagi Korban Kejahatan dan Penyalahgunaan Kekuasaan, 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.[[8]](#footnote-8) 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 kaitannya dengan konsumen, hukum melindungi hak-hak konsumen dari segala pelanggaran terhadap hak-hak tersebut.[[9]](#footnote-9) Dalam 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. Aspek hukum dari perkembangan ini juga hadir. Tingkat kecemasan klien akan dipengaruhi oleh perubahan sistem keamanan manajemen perusahaan dan unsur hukum. Standar yang ketat akan menjadi panduan untuk meningkatkan sistem keamanan, yang pada akhirnya akan mengurangi kecemasan pelanggan. Jika kita berbicara secara khusus tentang prinsip keamanan siber, maka pemutakhiran aplikasi mutlak diperlukan. 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, jangan lupakan pertimbangan-pertimbangan umum yang perlu diperhatikan 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 diatas maka dapat ditarik suatu rumusan masalah sebagai berikut:

* + - 1. Apa yang dimaksud dengan kejahatan terhadap sistem perbankan Indonesia di era cyberspace?
      2. Bagaimana upaya yang dapat dilakukan pemerintah, perbankan, masyarakat dalam menghadapi persoalan tersebut?

### Hasil Penelitian dan Pembahasan

Keamanan cyber adalah 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.[[10]](#footnote-10)Keamanan data dalam sistem informasi perbankan yang sangat canggih dan terkomputerisasi telah menjadi salah satu aspek penting dalam menjalankan sistem tersebut. Hal ini terutama disebabkan oleh fakta bahwa organisasi berbasis IT lebih mengutamakan informasi saat berurusan dengan kliennya.[[11]](#footnote-11) Karena ketergantungan yang tinggi terhadap teknologi informasi, kejahatan dunia maya semakin meningkat. Bank dan lembaga lain tidak menyadari bahwa mereka sedang memimpin era kejahatan internet meskipun mereka terus memperbarui sistem komputer mereka. Meningkatnya penggunaan komputer dan teknologi serta perangkat yang mudah digunakan seperti ponsel pintar, laptop, dan iPod telah memungkinkan lebih banyak ruang untuk memanfaatkan dan mengubah data. Oleh karena itu, hal yang paling penting bagi lembaga keuangan mana pun adalah melindungi aset informasi mereka dari orang-orang yang tidak jujur dan kecurangan sangat penting bagi lembaga keuangan. Saat ini, baik masyarakat awam maupun profesional menyalahgunakan teknologi. Oleh karena itu, 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.[[12]](#footnote-12) Oleh karena itu,menyatakan bahwa melindungi karyawan ini dari sistem informasi menjadi lebih sulit dan rumit karena mereka berasal dari dalam organisasi.[[13]](#footnote-13)

Karena informasi adalah aset berharga dan rahasia, maka pihak Bank harus mencegah orang lain mengaksesnya. Oleh sebab itu Bank sangat memperhatikan keamanan informasi. Maka terhadap pengendalian keamanan yang memadai harus terus ditinjau untuk mencegah aset dari digunakan, diungkapkan, diubah, atau dihancurkan secara tidak disengaja.[[14]](#footnote-14) 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:[[15]](#footnote-15)

* + - 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 mengkhawatirkan.[[16]](#footnote-16) 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.[[17]](#footnote-17) 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.[[18]](#footnote-18) 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.[[19]](#footnote-19)

Kejahatan dunia maya dibagi menjadi dua kategori. Jenis kejahatan pertama melibatkan penggunaan komputer sebagai sasaran kegiatan kriminal.[[20]](#footnote-20) sedangkan jenis kedua melibatkan penggunaan komputer sebagai alat. Pencurian informasi, peretasan, dan malware merupakan kejahatan yang paling sering terjadi di perbankan dibandingkan dua jenis kejahatan sebelumnya. Sasaran utama kejahatan ini adalah nasabah yang melakukan transaksi melalui Internet.[[21]](#footnote-21)

1. **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 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. Bank wajib mengembalikan seluruh uang nasabah karena tindakan tersebut menyebabkan uang nasabah hilang. 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. Merupakan tanggung jawab pemerintah untuk menciptakan lingkungan yang mendukung keamanan siber. 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.

Menurut pengamat bank Fadhil Hasan, langkah bank memberikan santunan kepada nasabah yang menjadi korban pencurian ATM merupakan langkah positif karena membebaskan korban dari risiko kehilangan dananya, namun langkah tersebut saja tidak cukup meredam keresahan masyarakat. mengenai perlindungan sumber dayanya pada sistem perbankan nasional. Jika pihak berwenang gagal untuk segera mengidentifikasi kasus-kasus pencurian dan administrator bank gagal meyakinkan masyarakat tentang sistem keamanan dana nasabah, keresahan masyarakat akan semakin kuat dan meluas. Jika hal ini terjadi, bank nasional harus menanggung risiko dampak kasus tersebut terhadap sistem.[[22]](#footnote-22)

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

1. **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:[[23]](#footnote-23)

a.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.

b.Menghilangkan atau tidak mencatat dalam akuntansi atau laporan, serta dalam dokumen atau laporan kegiatan komersial, transaksi atau rekening bank.

c. 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, Anda diancam dengan pidana penjara paling singkat 5 (lima) tahun dan paling lama 15 (lima belas) tahun.

Tentu hal tersebut juga dapat membuat peluang pemboloan rekening nasabah dimana 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 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.

1. **Faktor Dari Masyarakat**

Kejahatan terhadap sistem keamanan perbankan juga dapat ditinjau dari pidak masyarakat, dimana 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 dimana pelaku dapat memberikan berbagai upaya penawaran yang menarik sehingga masyarakat tergiur akan penawaran yang diberikan.

Ketiga, faktor budaya dimana budaya yang ada di masyarakat dapat memepengaruhi gaya hidup, cara hidup masyarakat di lingkungannya. Misal 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 satu nya apabila pelaku kejahatan cyber membagikan pesan dengan menyertakan link dimana 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 non-litigasi dan non-litigasi. Pentingnya memiliki aturan. Tujuannya lebih menitikberatkan pada upaya preventif dibandingkan aspek lainnya.Sebelumnya menimbulkan kerugian bagi konsumen karena rumitnya penyelidikan dan pengungkapan kejahatan dunia maya.[[24]](#footnote-24)

Meningkatkan kesadaran masyarakat adalah langkah awal untuk meningkatkan keamanan siber. Bagaimana pemerintah dapat mendidik masyarakat tentang praktik keamanan yang baik dan bahaya dunia maya, membuat inisiatif dan program yang akan memberdayakan masyarakat untuk mengatasi ancaman dunia maya dengan lebih baik.

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 profesional dan organisasi 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. Dibandingkan dengan perkembangan dan kebutuhan digital, Indonesia kekurangan talenta keamanan siber. Oleh karena itu, pemerintah diharapkan untuk fokus pada keamanan siber untuk mengatasi masalah privasi data.[[25]](#footnote-25)

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:[[26]](#footnote-26)

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).

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

Meningkatkan kesadaran masyarakat adalah langkah awal untuk meningkatkan keamanan siber. Bagaimana pemerintah dapat mendidik masyarakat tentang praktik keamanan yang baik dan bahaya dunia maya. Merupakan tanggung jawab pemerintah untuk menciptakan lingkungan yang mendukung keamanan siber. Pemerintah juga mempunyai tanggung jawab untuk menyediakan sumber daya dan pelatihan bagi masyarakat umum dan profesional TI untuk mengembangkan keterampilan keamanan siber. Bagaimana upaya dan sumber daya pelatihan ini dapat meningkatkan pengetahuan dan keterampilan yang diperlukan untuk melindungi diri kita dari ancaman dunia maya. Pemerintah dapat mendorong sektor swasta dan masyarakat menuju praktik keamanan yang lebih baik dengan menetapkan peraturan dan kebijakan yang tepat.Keberhasilan dalam menghadapi ancaman siber yang semakin meningkat bergantung pada kolaborasi antara pemerintah dan sektor swasta dalam hal ini adalah 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.

Sistem keamanan perbankan Indonesia harus selalu mutakhir dengan memasukkan fitur-fitur keamanan baru yang sesuai dengan kemajuan teknologi. Aspek hukum dari perkembangan ini juga hadir. Tingkat kecemasan klien akan dipengaruhi oleh perubahan sistem keamanan manajemen perusahaan dan unsur hukum. Standar yang ketat akan menjadi panduan untuk meningkatkan sistem keamanan, yang pada akhirnya akan mengurangi kecemasan pelanggan. Dalam kaitannya dengan prinsip keamanan siber, memperbarui aplikasi sangatlah penting. 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, jangan lupakan pertimbangan-pertimbangan umum yang perlu diperhatikan dalam melakukan pembaruan aplikasi, seperti memastikan ketersediaan layanan, menjaga stabilitas sistem elektronik, dan meningkatkan keamanan sistem terhadap berbagai ancaman siber.

### 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. Banyak sekali kejahatan cyber di bidang perbankan yang bekaitan dengan sistem keamanan perbankan, diantara nya kejahatan carding “*credit card fraud”*, ATM atau EDC “skimming”, hacking, cracking, phising “i*nternet banking fraud*”, malware “*virus/worm/trojan/bots*”, cybersquatting, pornografi, perjudian online, transnasional crime “perdagangan narkoba, mafia, terorisme, *money laundering, human trafficking, underground economy*”. Ada beberapa yang menjadi penyebab terjadinya kejahatan cyber terhadap sistem keamanan perbankan yang pertama ada faktor dari pemerintah, kedua dari pihat swasta (Bank), ketiga dari pihak masyarakat. faktor dari pemerintah pertama, lemah nya regulasi yang ada saat ini sehingga masih terjadi banyak kejahatan sistem kemanan perbankan. Kedua, sering berubah-ubahnya regulasi juga menjadi salah satu faktor terjadinya kejahatan terhadap sistem keamanan perbankan. Ketiga, di Indonesia sendiri tim reaksi cepat untuk menindaklanjuti serangan-serangan siber yang terjadi masih belum efektif. Keempat, Kurangnya peran Pemerintah dalam bertindak dengan menyediakan sumber daya dan pelatihan bagi masyarakat dan profesional IT untuk membangun kemampuan keamanan siber. Dari faktor swasta pertama, karena kegagalan sistem. Kedua, terdapat beberapa kelalaian yang disengaja dari pihak perbankan. Ketiga, Kurang memadai fasilitas yang ada di masyarakat. Dari faktor masyarakat

Meningkatkan kesadaran masyarakat adalah langkah awal untuk meningkatkan keamanan siber. Bagaimana pemerintah dapat mendidik masyarakat tentang praktik keamanan yang baik dan bahaya dunia maya. Merupakan tanggung jawab pemerintah untuk 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 keamanan siber. Bagaimana upaya dan sumber daya pelatihan ini dapat meningkatkan pengetahuan dan keterampilan yang diperlukan untuk melindungi diri kita dari ancaman dunia maya. Pemerintah dapat mendorong sektor swasta dan masyarakat menuju praktik keamanan yang lebih baik dengan menetapkan peraturan dan kebijakan yang tepat.Keberhasilan dalam menghadapi ancaman siber yang semakin meningkat bergantung pada kolaborasi antara pemerintah dan sektor swasta dalam hal ini adalah 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, Urgensi Perlindungan Korban Kejahatan (Antara Norma Dan Realita). Jakarta: PT. Raja Grafindo Persada, 2006.

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

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

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

**Jurnal**Ardiyanti, H. Cyber-security dan tantangan pengembangannya di indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional,2016.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. Kejahatan Siber dalam Bidang Perbankan. Cyber Security Dan Forensik Digital, Vol.I. No.2, 2018.

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.VI. No.1. Juni. 2021.

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

Kaiser, R. “Lahirnya Perang Cyber.” Geografi Politik. 2015. 46.

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, Oktober 2021.

Librianty, A., 2015. *Mengenal Modus Pembobolan ATM Melalui Teknik Skimming*. [Online] Available at: http://tekno.liputan6.com/read/2302264/me ngenal-modus-pembobolan-atm-melalui- teknik-skimming [Accessed 8 Januari 2024].

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

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

Martin, JC. Layanan Kepercayaan: Cara yang Lebih Baik untuk Mengevaluasi Kontrol TI. *Jurnal Akuntansi, 2005.* 199 (3).

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

Muhammad Khairul Faridi. Kejahatan Siber Dalam Perbankan. CyberSecurity dan Forensik Digital Vol. 1, No. 2, November 2018.

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

Ronny Prasetya, “Pembobolan ATM: Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan”, Jakarta: Prestasi Pustaka. 2010.

Ronny Prasetya, Pembobolan ATM, Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan (Jakarta: PT. Prestasi Pustakaraya, 2010).

Rudiatno, Aldea Mita Cheryta.

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.

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

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

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.

1. Kaiser, R. 2015. “Lahirnya Perang Cyber.” Geografi Politik 46: hlm.11–20. [↑](#footnote-ref-1)
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.VI. No.1. Juni. 2021. hlm.7-8. [↑](#footnote-ref-2)
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, hlm.2-3. [↑](#footnote-ref-3)
4. Muhamad Djumhana, Hukum Perbankan di Indonesia. Bandung: PT. Citra Aditya Bakti. 2021. hlm.8-9. [↑](#footnote-ref-4)
5. Ibid. hlm.11. [↑](#footnote-ref-5)
6. Muladi, & Barda Nawawi Arief. Bunga Rampai Hukum Pidana, Cetakan Pertama. Bandung: Alumni. 1992. hlm.63. [↑](#footnote-ref-6)
7. Ronny Prasetya, “Pembobolan ATM: Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan”, Jakarta: Prestasi Pustaka. 2010. hlm.5. [↑](#footnote-ref-7)
8. Dikdik M. Arief Mansur dan Elisatris Gultom, Urgensi Perlindungan Korban Kejahatan (Antara Norma Dan Realita) (Jakarta: PT. Raja Grafindo Persada, 2006). hlm. 23-24. [↑](#footnote-ref-8)
9. Mochammad Najib Imanullah Zennia Almaida, “Perlindungan Hukum Preventif Dan Represif Bagi Pengguna Uang Elektronik Dalam Melakukan Transaksi Tol Nontunai,” Private Law 9, no. 1 (2021): 222, [↑](#footnote-ref-9)
10. Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional,2016.Vol.X.No.1. hlm.7. [↑](#footnote-ref-10)
11. Martin, JC. Layanan Kepercayaan: Cara yang Lebih Baik untuk Mengevaluasi Kontrol TI. *Jurnal Akuntansi, 2005.* 199 (3). [↑](#footnote-ref-11)
12. Loch, Karen D., Houston H. Carr dan Merrill E. Warkentin. Ancaman terhadap sistem informasi: Realitas hari ini, pemahaman kemarin. *MIS Triwulanan, 1992. Hlm.*173 - 186. [↑](#footnote-ref-12)
13. Whitman, SAYA (2004). Dalam membela dunia: memahami ancaman terhadap keamanan informasi. *Jurnal Internasional Manajemen Informasi,* 24 (1), 2004. hlm.43-57. [↑](#footnote-ref-13)
14. 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) 199 – 204. [↑](#footnote-ref-14)
15. Rudiatno, Aldea Mita Cheryta. [↑](#footnote-ref-15)
16. Handrini Ardiyanti. Cyber Security Dan Tantangan Pengembangannya. Pengolahan Data dan Informasi Sekretariat Jenderal DPR RI: Politicia. Vol.X No.1. 2014. [↑](#footnote-ref-16)
17. Marcelina, D., Suryati, & Yulianti, E. Workshop Teknologi Informasi “Dasar Cyber Security” Pada SMK PGRI Tanjung Raja Ogan Ilir (OI). *Jurnal Abdimas Mandiri. Vol.VI.No. 2. 2022. hlm.* 67-72. [↑](#footnote-ref-17)
18. Suharto, M. A., & Apriyani, M. N. Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Jurnal RisalahHukum, Vol.XVII, No.2. 2021*, hlm.98-107. [↑](#footnote-ref-18)
19. Faridi, M. K. Kejahatan Siber dalam Bidang Perbankan. Cyber Security Dan Forensik Digital, Vol.I. No.2, 2018. hlm.57–61. [↑](#footnote-ref-19)
20. Librianty, A., 2015. *Mengenal Modus Pembobolan ATM Melalui Teknik Skimming*. [Online] Available at: http://tekno.liputan6.com/read/2302264/me ngenal-modus-pembobolan-atm-melalui- teknik-skimming [Accessed 8 Januari 2024]. [↑](#footnote-ref-20)
21. Muhammad Khairul Faridi. Kejahatan Siber Dalam Perbankan. CyberSecurity dan Forensik Digital Vol. 1, No. 2, November 2018, hlm 57-61 [↑](#footnote-ref-21)
22. Ronny Prasetya, Pembobolan ATM, Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan (Jakarta: PT. Prestasi Pustakaraya, 2010). hlm. 40. [↑](#footnote-ref-22)
23. [↑](#footnote-ref-23)
24. 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, Oktober 2021 [↑](#footnote-ref-24)
25. Jayawickrana, Nihal. 2002.The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence. United Kingdom: Cambridge University Press. [↑](#footnote-ref-25)
26. Dwikari Nuristiningsih, 2023, Upaya Penal Dan Non Penal Dalam Menanggulangi Tindak Pidana Teknologi Informasi, Vol.XXIII, No.2, hlm.88. [↑](#footnote-ref-26)