Jurnal Publikasi Ekonomi dan Akuntansi
Volume 5 Nomor 3 September 2025
E-ISSN : 2808-9006; P-ISSN 2808-9391, Hal 472-479
DOI: https://doi.org/10.51903/jupea.v5i3.4328
Available online at: https://journalcenter.org/index.php/jupea

Perlindungan Hukum Nasabah Pada Era Digital : Menyikapi Ancaman Kejahatan Siber Di Sektor Perbankan

Nia Malvin Faradila[1*], Baidhowi[2]
[1,2]Universitas Negeri Semarang
Email: niamalvinfrdl@students.unnes.ac.id, baidhowi@mail.unnes.ac.id

Alamat: Sekaran, Kec. Gn. Pati, Kota Semarang, Jawa Tengah 50229
**Korespondensi penulis: niamalvinfrdl@students.unnes.ac.id*

Abstract. *The rapid digital transformation has succeeded in providing significant benefits to the banking world, it is expected to be able to help the banking sector in providing better services to customers and competing with technology in the industry 4.0 era. But besides that, digital transformation also creates a great opportunity for crime risks, such as skimming, phishing, social engineering, and malware that can threaten the security of customers.There are several problem formulations that will be discussed in this article, namely: (1) How do cybercriminals steal customer data in the banking sector? and (2) How is the legal system in overcoming criminal acts of data theft of bank customers? This article aims to analyze how the role of current regulations in dealing with legal problems experienced by the banking world in the digital era.To respond to the formulation of these problems, the author uses normative legal research by covering conceptual approaches, statutory approaches, and collecting data through literature studies.This research is expected to provide useful knowledge to help develop theory and practice in the field of banking digitalization and consumer protection.*
Keywords*: Personal data protection; banking law; digital transformation*

Abstrak. Transformasi digital yang amat pesat telah berhasil memberikan manfaat yang signifikan terhadap dunia perbankan, hal tersebut diharapkan mampu membantu sektor perbankan dalam memberikan pelayanan yang lebih baik kepada nasabah serta bersaing dengan teknologi di era industry 4.0. Namun disamping itu, transformasi digital juga menimbulkan adanya peluang besar terjadinya resiko kejahatan, seperti skimming, phising, social engineering, serta malware yang dapat mengancam keamanan para nasabah.Terdapat beberapa rumusan masalah yang akan dibahas dalam artikel ini, yaitu: (1) Bagaimana cara cybercriminal mencuri data para nasabah di sektor perbankan? dan (2) Bagaimana sistem hukum dalam menanggulangi tindak pidana pencurian data para nasabah bank?.Artikel ini bertujuan untuk menganalisis bagaimana peran regulasi saat ini dalam menangani permasalahan hukum yang dialami oleh dunia perbankan pada era digital.Untuk menanggapi rumusan masalah tersebut, penulis menggunakan penelitian hukum normatife dengan meliputi pendekatan konseptual, pendekatan perundang-undangan, dan mengumpulkan data melalui studi kepustakaan.Penelitian ini diharapkan dapat memberikan ilmu pengetahuan yang berguna untuk membantu pengembangan teori serta praktik dalam bidang digitalisasi perbankan. dan perlindungan konsumen.
Kata kunci: Perlindungan data pribadi; hukum perbankan; transformasi digital

1. LATAR BELAKANG

Pemanfaatan teknologi digital dan internet yang luas menandai dimulainya era industri 4.0, yang merupakan fase transformasi yang signifikan dalam berbagai aspek kegiatan industri dan kehidupan manusia. Konsep ini mencakup proses produksi yang terorganisir menggunakan teknologi nirkabel dan big data, yang memungkinkan pengelolaan data yang lebih baik di sistem server. Semua proses diaktifkan untuk beroperasi secara otomatis dalam satu sistem yang terpadu. Kemajuan teknologi juga didukung dengan adanya perkembangan internet yang semakin pesat, menjadi katalisator utama untuk berbagai inovasi baru di segala aspek kehidupan manusia, terutama dalam sektor perbankan.

Dunia perbankan global saat ini berada dalam fase transformasi yang sangat pesat, terutama dengan munculnya perbankan digital sebagai komponen utama yang memungkinkan lembaga keuangan bersaing di tengah ketatnya persaingan di sektor keuangan. Digitalisasi dalam sektor ini telah menjadi suatu kebutuhan yang mendesak, tidak hanya untuk memenuhi harapan konsumen yang terus berkembang, tetapi juga untuk menghadapi tantangan dari perusahaan teknologi finansial (fintech) yang semakin dominan.Dengan semakin

Diterima: 11 Juni 2025; Direvisi: 20 Juni 2025;Disetujui: 22 Juli 2025;Tersedia Online: 14 Agustus 2025; Diterbitkan: 8 September 2025

meningkatnya penggunaan teknologi informasi, bank-bank harus beradaptasi dengan perubahan perilaku nasabah yang kini lebih memilih layanan yang cepat, efisien, dan mudah diakses. Hal ini mendorong lembaga perbankan untuk mengadopsi inovasi seperti mobile banking dan aplikasi berbasis web yang memungkinkan transaksi dilakukan kapan saja dan di mana saja. Selain itu, digitalisasi juga berkontribusi pada peningkatan efisiensi operasional, di mana otomatisasi proses bisnis dapat mengurangi biaya dan mempercepat layanan.

Dengan semakin banyaknya penggunaan teknologi informasi, bank-bank harus beradaptasi dengan perubahan perilaku nasabah yang kini lebih memilih layanan yang cepat, efisien, dan mudah diakses. Hal ini mendorong lembaga perbankan untuk mengadopsi inovasi seperti mobile banking dan aplikasi berbasis web yang memungkinkan transaksi dilakukan kapapun dan dimanapun. Selain itu, digitalisasi juga berkontribusi pada peningkatan efisiensi operasional, di mana otomatisasi proses bisnis dapat mengurangi biaya dan mempercepat layanan.Namun, di balik manfaat yang diberikan oleh perbankan digital, terdapat tantangan serta risiko hukum yang perlu diselesaikan. Perlindungan data dan privasi pelanggan adalah prioritas utama karena kejahatan siber seperti peretasan data, pencurian identitas, dan peretasan informasi pribadi semakin meningkat. Selain itu, pengawasan ketat diperlukan karena banyaknya penipuan elektronik, pencucian uang, dan praktik perbankan digital yang tidak etis.Apabila tidak ditangani dengan benar, maka risiko ini tidak hanya dapat merugikan nasabah secara pribadi, tetapi juga dapat mengancam stabilitas sistem keuangan secara keseluruhan.

Regulasi perbankan di era digital harus mengikuti kemajuan teknologi dan mangatasi masalah yang muncul.Pengaturan yang efisien dan fleksibel sangat penting untuk stabilitas sektor perbankan, mengurangi risiko hukum, dan meningkatkan kepercayaan nasabah. Regulasi yang baik tidak hanya berfokus terhadap upaya untuk mengurangi risiko, tetapi juga mendukung kemajuan teknologi dalam industri perbankan.Hal tersebut bertujuan agar perkembangan teknologi dapat digunakan secara optimal tanpa mengorbankan kepercayaan dan keamanan publik.Adanya regulasi yang adaptif, industri perbankan diharapkan dapat mengatasi berbagai tantangan di era digital, menciptakan lingkungan yang aman bagi semua pihak, serta mampu menjaga kepercayaan nasabah terhadap layanan yang diberikan.Regulasi mengenai pencurian data pribadi di sektor perbankan di Indonesia telah tercantum dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Selain regulasi, praktik keamanan terbaik dalam pengelolaan data dan sistem dalam industry perbankan juga memiliki peran yang sangat penting untuk menjaga keamanan data para nasabah, yang mana sudah termasuk mengenai pelatihan karyawan tentang praktik keamanan siber, penggunaan enkripsi yang kuat, serta melakukan audit keamanan secara rutin. Bank juga harus melakukan transparansi mengenai bagaimana cara mereka dalam menggabungkan, menggunakan, dan menjaga data para nasabah, serta memberikan hak kepada para nasabah untuk mengontrol informasi mereka.

Berdasarkan latar belakang yang telah diuraikan sebelumnya, muncul rumusan masalah, yaitu: (1) Bagaimana cara cyber criminal mencuri data para nasabah di sektor perbankan? dan (2) Bagaimana sistem hukum dalam menanggulangi tindak pidana pencurian data para nasabah bank?.Artikel ini bertujuan untuk menganalisis bagaimana peran regulasi saat ini dalam menangani permasalahan hukum yang dialami oleh dunia perbankan pada era digital.Untuk menanggapi rumusan masalah tersebut, penulis menggunakan penelitian hukum normatife dengan meliputi pendekatan konseptual, pendekatan perundang-undangan, dan mengumpulkan data melalui studi kepustakaan.

2. KAJIAN TEORITIS

Transformasi Digital dan Risiko Kejahatan Siber dalam Perbankan

Transformasi digital dalam sektor perbankan adalah komponen resolusi industri 4.0 yang diperlihatkan dengan adanya penggunaan teknologi digital, big data, dan internet untuk meningkatkan efesiensi pelayanan dan daya saing lembaga keuangan.Dengan mengadopsi inovasi seperti aplikasi berbasis web, mobile banking, serta proses bisnis yang otomatis, hal tersebut memungkinkan adanya transaksi yang dapat dilakukan secara real time dan tepat waktu sekaligus memperhitungkan biaya operasional.

Akan tetapi, kemajuan ini juga menimbulkan resiko baru berupa kejahatan siber.Berdasarkan Teori Cybercrime dijelaskan bahwa, digitalisasi terbukti dapat memperbesar serangan serta menciptakan kesempatan baru terhadap pelaku kejahatan untuk mengeksploitasi kelemahan sistem.Dalam konteks perbankan terdapat ebberapa jenis kejahatan siber antara lain yaitu keylogger, skimming, botnet, malware, phising, backdoor, rootkit, dan sebagianya.

Teori Perlindungan Data Pribadi dan Hukum Perbankan

Teori ini menegaskan mengenai pentingnya keamanan data dan hak privasi sebagai komponen hak asasi manusia yang harus dijunjung tinggi oleh bangsa penegakan hukum dan regulasi yang efektif.Di Indonesia perlindungan privasi sendiri telah diatur pada Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan beberapa regulasi sektoral lainnya di industri perbankan.

Selain itu, Teori *law as a tool of social engineering (Roscoe Pound)* juga relavan, yaitu hukum harus mampu menyesuaikan diri dengan perubahan teknologi dan sosial untuk menegakkan hak-hak masyarakat dan melindungi kepentingan mereka. Sehubungan dengan hal tersebut maka regulasi perbankan digital selalu diperbarui untuk mencegah munculnya kejahatan baru serta memperjelas tanggung jawab lembaga keuangan dan penyedia layanan teknologi.

3. METODE PENELITIAN

Metodelogi dalam artikel ini menggunakan jenis penelitian hukum normatif yang berfokus terhadap pendekatan perundang-undangan serta pendekatan konseptual. Sumber bahan hukum primer yang digunakan yaitu Undang-Undang Nomor 19 tahun 2016 mengenai Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan Undang-Undang Nomor 3 Tahun 2011 Tentang Transfer Dana, Undang-Undang Nomor 21 tahun 2011 tentang Otoritas Jasa Keuangan, serta Kitab Undang-Undang Hukum Pidana.Kemudian, bahan hukum sekunder yang digunakan yaitu kamus hukum dan jurnal, hasil penelitian, dan tulisan ilmiah untuk menudukung artikel ini.

Metode pengumpulan data yang digunakan dalam penelitian ini adalah studi kepustakaan, yang melibatkan analisis konten yang relevan, seperti buku, peraturan perundang-undangan, dokumen, dan hasil penelitian yang terkait atau sebanding dengan masalah yang diteliti. Tujuan dari metode ini adalah untuk mendapatkan informasi dan memperoleh pemahaman yang lebih baik mengenai permasalahan yang sedang diteliti.

4. HASIL DAN PEMBAHASAN

Bagaimana Cara Cybercriminal Mencuri Data Para Nasabah Di Sektor Perbankan ?

Hukum dan Masyarakat merupakan dua hal yang saling berhubungan, oleh sebab itu agar hukum dapat tetap berjalan dengan efektif maka hukum dan masyarakat harus sama-sama berkembang.Seiring dengan adanya perkembangan teknologi di masyarakat hal ini akan menimbulkan berbagai jenis kejahatan baru, semain bertambah khususnya cyber crime.

Regulasi mengenai perbankan harus mampu mengitu perkembangan teknologi serta melaindungi seluruh pihak yang telibat dalam sektor perbankan untuk menangani tantangan

hukum yang sedang dihadapi oleh sektor perbankan di era digital.Privasi dan keamanan data para nasabah merupakan tantangan utama yang terjadi dalam sektor perbankan. Serangan hacking dan peretasan data dapat mengakibatkan kerugian yang besar bagi para nasabah dan Lembaga keuangan.

Transformasi digital merupakan katalisator utama pemicu terjadinya berbagai jenis cyber crime di sektor perbankan, akan tetapi pada kenyataanya terdapat sejumlah faktor lainnya yang menjadi pemicu terhadap meingkatnya cyber crime yaitu lemahnya infrastruktur teknologi dan enkripsi data, adanya penyimpanan akses ketat seperti akses tidak sah ke system bank, serta masih terdapat banyak bank yang bergantung terhadap penyedia layanan teknologi eksternal.

Pelanggaran sistem keamanan tersebut tidak hanya berdampak pada bank secara finansial dan reputasi, tetapi juga menempatkan nasabah dalam posisi rentan terhadap ancaman seperti pencurian identitas, penipuan, dan penyalahgunaan data.

Jenis-jenis cyber crime yang terjadi tersebut meliputi :

a. Sniffing

Suatu Teknik yang dilakukan oleh pelaku dengan cara menganalisis serta memantau paket data yang dikirimkan lewat jaringan internet.Cara kerja sniffing yaitu dengan mengintersepsi data yang dikirim antara server dan komputer pengguna yang umumnya sering terjadi terhadap jaringan yang tidak terenkripsi atau memeiliki tingkat keamanan rendah, contohnya jaringan Wi-Fi yang digunakan secara publik.

b. Web Deface: System Exploitation

Suatu tindakan mengubah beranda depan suatu situs resmi untuk merusak situs, menunjukkan kerawanan keamanan situs dan menyebarkan pesan yang berisi kebohongan tertentu.

c. Virus, Worm, Trojan

Tipe software yang digunakan untuk memanipulasi informasi, merusak system computer, mencuri data, serta tindakan kejahatan lainnya untuk menguntungkan pelaku.

d. Denial of Service

Suatu penyerangan berupa pengiriman sejumlah besar data atau permintaan ke jaringan atau server korban dalam waktu cepat, sehingga hal tersebut mengakibatkan system menjadi lamban bahkan tidak dapat diakses sama sekali karena telah lebih dari kapasitas normal.

e. Key Logger

Program atau perangkat lunak yang telah diatur agar dapat mencatat setiap huruf yang diketik pada keyboard.Cara kerja Key Logger yaitu dengan cara merekam diam-diam segala aktivitas yang diketik pada keyboard, seperti kata sandi, nomor telepon, identitas pengguna, dll yang nantinya akan disalahgunakan oleh pelaku.

f. Typo Site

Suatu situs web palsu dengan Alamat IP dan nama domain yang dibuat menyerupai situs asli yang bertujuan untuk membuat para pengguna internet salah dalam mengetik pada saat melakukan pencarian alamat situs yang akan mereka gunakan.

Jenis-jenis cyber crime yang telah dijelaskan sebelumnya tersebut dapat diterapkan pada modus operandi yang biasanya digunakan untuk kejahatan pencurian data pribadi di sektor perbankan, sebagai berikut :

a. Carding

Tindakan mencuri data kartu kredit yang kemudian digunakan untuk melakukan jual beli secara ilegal pada situs belanja online dan hal tersebut umumnya dilakukan dengan memperoleh informasi kartu kredit korban secara tidak sah, seperti pencurian data, penipuan , atau kebocoran data.

b. Malware

Tindakan tersebut umumnya dilakuakn untuk meretas sebuah perangkat atau website sehingga daapat diakses bebas dengan mudah.Hal tersebut juga sering digunakan untuk mencuri data pengguna internet.Sehingga malware sudah dianggap biasa untuk digunakan sebagai alat mencuri data nasabah perbankan untuk mengambil uang dari rekening sampai menggunakan kartu kredit.

Jenis-jenis Malware :

a. Botnet

Menginstall diri ke dalam komputer untuk memberikan akses kepada penyerang, memungkinkan penyerang untuk terhubung ke komputer dengan sedikit atau tanpa autentikasi, dan menjalankan perintah-perintah pada sistem lokal.

b. Pencurian Informasi

Mengumpulkan informasi dari komputer korban dan mengirimkannya kepada penyerang. Contoh: sniffers, pengambil hash kata sandi, dan keyloggers

c. Rootkit

Dimaksudkan untuk menyembunyikan keberadaan kode lain, biasanya dipasangkan dengan malware lain, seperti backdoor, untuk memberikan akses jarak jauh kepada penyerang dan membuat kode sulit terdeteksi oleh korban.

d. Backdoor

Yaitu menginstall diri ke dalam komputer untuk memberikan akses kepada penyerang, memungkinkan penyerang untuk terhubung ke komputer dengan sedikit atau tanpa autentikasi, dan menjalankan perintah-perintah pada sistem lokal.

e. Phising

Suatu tindakan mengirimkan pesan palsu melalui website, email, chat, dll yang dilakukan untuk untuk mendapatkan informasi pribadi para pengguna gadget.

Kejahatan di bidang perbankan yang dahulu kerapkali dilakukan secara nyata dan langsung seperti, perampokan bank atau pemalsuan dokumen yang mana pada zaman sekarang dapat dilakukan secara virtual tanpa adanya batas ruang maupun waktu.Perubahan tersebut mendesak agar sistem pengaturan hukum juga berkembang sesuai dengan perkembangan zaman serta teknologi.Undang-Undang yang ada perlu diperbarui dan disesuaikan untuk menangani permasalahan baru yang dihadapi oleh sektor perbankan akibat kejahatan siber.

Bagaimana Sistem Hukum Dalam Menanggulangi Tindak Pidana Pencurian Data Para Nasabah Bank?

Pada era digitalisasi, teknologi informasi dan komunikasi telah menjadikan segalanya serba efektif karena memungkinkan akses tanpa batas, ruang, waktu, dan jarak, yang berdampak pada pola kehidupan masyarakat serta mendukung perubahan ekonomi, sosial, budaya, keamanan, dan penegakan hukum.Oleh karena itu, peraturan yang berlaku untuk melindungi masyarakat di era digitalisasi harus diperketat karena lebih sensitif terhadap perubahan sosial, ekonomi, budaya, dan penegakan hukum.

Perlindungan terhadap data pribadi para nasabah bank Indonesia merupakan hal yang semakin penting, khususnya dengan adanya semakin cepat kemajuan teknologi digital yang dapat mengubah cara orang dalam melakukan transaksi keuangan.Bank memiliki tanggung jawab untuk menjaga data pribadi nasabah aman. Selain itu, mereka juga berkwajiban untuk memastikan bahwa data tersebut aman serta tidak disalahgunakan.

Hal tersebut selaras dengan tujuan yang termaktub dalam Pembukaan UUD RI 1945, khususnya pada alinea keempat, dengan memberikan jaminan hukum mengenai kehadiran Bank Digital untuk melindungi para nasabahnya, melindungi seluruh warga negara Indonesia, serta mengutamakan kesejahteraan umum merupakan tujuan utamanya.Pasal 28 G ayat (1) Undang-Undang Dasar 1945 menjelaskan tujuan ini dengan menyatakan bahwa setiap orang berhak atas perlindungan keluarga, diri sendiri, harta benda, martabat, serta

kehormatan yang berada di bawah kekuasaannya, serta atas rasa aman dan perlindungan dari ancaman rasa takut, yang termasuk hak asasi manusia.

Lembaga Otoritas Jasa Keuangan (OJK) telah menerbitkan regulasi baru yaitu Peraturan Otoritas Jasa Keuangan (OJK) Nomor 12/POJK.03/2021 mengenai Bank Umum yang merupakan salah satu aturan yang bertujuan untuk melindungi perbankan digital sebagai bagian dari revolusi industri 4.0 dan 5.0.Kemudian, untuk menyempurnakan regulasi mengenai bank digital, OJK juga menerbitkan Peraturan OJK terbaru Nomor 13/POJK.03/2021 mengenai Penyelenggaraan Produk Bank Umum serta Peraturan OJK Nomor 14/POJK.03/2021 sebagai bentuk Perubahan terhadap Peraturan OJK Nomor 34/POJK.03/2018 terkait Penilaian Kembali Pihak Utama Lembaga Jasa Keuangan.

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Jasa Keuangan menetapkan tanggung jawab bank untuk melindungi data pribad nasabah. Pasal 40 ayat (1) mengatur rahasia bank, yang mewajibkan bank untuk menjaga kerahasiaan data nasabah dan simpanannya. Menurut Pasal ini, bank digital bertanggung jawab untuk menjaga data pribadi dan dana pelanggan. Selain itu, Pasal 40 A menyatakan bahwa bank diperbolehkan untuk memberikan informasi tentang nasabah jika ada keperluan peradilan, seperti dalam perkara perdata, penyelesaian piutang bank, atau atas permintaan pelanggan sendiri.

Kebijakan hukum pidana merupakan salah satu bagian dari upaya untuk penanganan tindak pidana pencurian data nasabah bank.Kebijakan tersebut yaitu berupa sanksi bagi siapapun yang melanggar undang-undang serta pencegahan dan penanggulangan kejahatan secara keseluruhan.Hal tersebut sesuai dengan pendapat Marc Ancel yaitu bahwa untuk menangani suatu kejahatan modern secara efektif, maka perlu diterapkannya suatu kebijakan hukum pidana harus holistik serta meliputi strategi pencegahan proaktif.

Kebijakan Penal

Beberapa kebijakan penal yang telah dilaksanakan untuk menangani kasus pencurian data pribadi di sektor perbankan antara lain sebagai berikut :

a. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Undang-Undang tersebut berisi mengenai perlindungan nasabah dan operasional terhadap sektor perbankan di Indonesia.

b. Undang-Undang Nomor 24 Tahun 2004 tentang Lembaga Penjamin Simpanan (LPS).

Undang-Undang ini berisi tentang lembaga yang ber- kewajiban untuk menjaga kepercayaan nasabah terhadap sistem perbankan Indonesia.

c. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK)

Undang-undang tersebut berisi mengenai regulasi serta pengawasan terhadap industri jasa keuangan (perbankan) di Indonesia.OJK dalam hal ini memiliki tanggung jawab untuk menjaga sistem keuangan tetap stabil serta melindungi keamanan data pribadi nasabah.

d. Undang-Undang Nomor 19 Tahun 2016 merupakan hasil dari Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

Undang-Undang tersebut berisi tentang tata cara pemanfaatan teknologi informasi dan transaksi elektronik, selain itu juga bertujuan untuk menjaga keamanan dan data pribadi, termasuk data yang di simpan oleh lembaga keuangan

e. Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah

Undang-Undang tersebut berisi tentang mekanisme serta perlindungan terhadap nasabah pada sektor perbankan syariah di Indonesia.

Kebijakan Non-Penal

Penanganan kasus pencurian data pribadi di sektor perbankan juga dapat dilakukan melalui pendekatan Non-Penal, yaitu tanpa melalui sanksi atau hukuman pidana, contohnya sebagai berikut :

a. Harmonisasi Hukum

Untuk memastikan kejahatan cyber dapat diatasi secara efektif melalui berbagai undang-undang, peraturan, dan persetujuan antar negara harus disesuaikan.

b. Pelatihan Personil terhadap Para Penegak Hukum

Memberikan pelatihan kepada personel penegak hukum agar mereka memiliki pengetahuan serta keterampilan yang mencukupi dalam menangani kejahatan cyber.

c. Pengembangan Teknologi serta Jaringan Informasi

Pembangunan sistem jaringan informasi yang kuat dan dapat diandalkan, seperti program "24 jam point contact", yang dimaksudkan untuk membantu negara berkolaborasi dan berkomunikasi dengan cepat dalam menangani ancaman cyber.

d. Penyebarluasan Kesepakatan Internasional

Menyebarluaskan serta menerapkan kesepakatan internasional mengenai kejahatan cyber untuk mewujudkanm prosedur serta standar konsisten di seluruh dunia.

Penegakan Hukum Pidana Kerjasama antar negara untuk menegakkan hukum yang bertujuan untuk menangkap dan memberikan hukuman kepada para pelaku kejahatan cyber, termasuk mekanisme ekstradisi dan bantuan hukum timbal balik.

5. KESIMPULAN DAN SARAN

Transformasi dalam industri perbankan Indonesia telah meningkatkan efisiensi operasional dan kualitas layanan pelanggannya. Namun, proses digitalisasi ini digitalisasijelas membuat pengguna rentan terhadap ancaman dunia maya yang semakin kompleks, seperti phishing, malware, media sosial , dan skimming, yang sering kali mengeksploitasi keamanan infrastruktur, standar pengkodean data, dan kerugian finansial bagi perusahaan ketiga.Proses tersebut secara gamblang memaparkan pengguna terhadap ancaman siber yang makin kompleks, seperti phishing, malware, media sosial, dan skimming, yang sering kali mengeksploitasi keamanan infrastruktur , standar pengkodean data, dan kerugian finansial bagi perusahaan ketiga dari sniffing dan perusakan web hingga botnet dan rootkit, menunjukkan bahwa orang terus beradaptasi dengan teknologi baru sambil mengurangi ancaman yang terus meningkat .

Dampak serangan siber has the Because Regulasi perlu diawasi secara ketat guna mencegah bentuk - bentuk kejahatan baru, meningkatkan standar keamanan siber di lembaga perbankan, dan menjelaskan peran lembaga keuangan serta penyedia layanan eksternal dalam melindungi data Nasabah. Dengan persyaratan dan pengawasan yang ketat, transformasi digital dapat menjadi sedikit lebih efektif yang digunakan oleh komunitas siber.

DAFTAR REFERENSI

A. S. , G., S. , L., & K. , N. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law, 1*(2), 68–81.

Aqila, A. E., & Suwarsit, A. (2024). Peran Regulasi Modern dalam Menjaga Integritas Sistem Hukum Perbankan Digital . *Jurnal Multidisiplin Ilmu Akademik, 1*(6), 229.

Cloudmatika. (2022, Juli 15). *Apa Itu Malware? Pengertian dan Contoh Virus Malware* . Retrieved Maret 24, 2025, from Cloudmatika: https://cloudmatika.co.id/blog-detail/apa-itu-malware

D. A. S., I. (2022). Data Privasi dan Keamanan Siber pada SmartCity . *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi, 2*(1), 54.

Ida, M. (2021). Menilik Financial Technology Dalam Bidang Perbankan . *Jurnal SOMASI (Sosial Humaniora Komunikasi), 2*(1), 32–43.

Kemal, B. I., Aulia, R. H., & Frygyta, D. S. (2024). Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital . *YUSTITIABELEN, 10*(2), 106.

M. J. , H., S. , S., Y. Y. , S., I. A. , R., S. , U., & S. R. , R. (2024). Sosialisasi Kebijakan Bank Digital: Perlindungan Hukum Terhadap Data Nasabah Dari Risiko Serangan Siber. *RENATA: Jurnal Pengabdian Masyarakat Kita Semua, 2*(2), 170.

M. R., T., & R. , A. (2020). Transformasi budaya organisasi otoritas perpajakan indonesia menghadapi era ekonomi digital. *Jurnal Aplikasi Bisnis Dan Manajemen (JABM), 5*(2), 253-253.

Perhimpunan, B. N. (2024, Oktober 26). *Ini Jenis-Jenis Kejahatan Digital Perbankan dan Tips Menghindarinya!* Retrieved Maret 24, 2025, from Perhimpunan Bank Nasional: https://perbanas.org/publikasi/artikel-perbanas/ini-jenis-jenis-kejahatan-digital-perbankan-dan-tips-menghindarinya

R. , A., R. F., R., L. O. A., D., A., P., Y. W., S., A. S., L., & N. , H. (2024). Transformasi Digital dan Antisipasi Perubahan Ekonomi Global dalam Dunia Perbankan. *MARAS: Jurnal Penelitian Multidisiplin, 2*(1), 80-8.

Rika, A. (2021, November 11). *Pahami Jenis-jenis Kejahatan Siber di Sektor Perbankan*. Retrieved Maret 24, 2025, from Bisnis.com: https://finansial.bisnis.com/read/20211111/90/1464684/pahami-jenis-jenis-kejahatan-siber-di-sektor-perbankan

Rizka, A., Renava, A., & Yowa Selvia Bayu Mustika. (2024). Perlindungan Konsumen dalam Era Digitalisasi Perbankan Bagi Konsumen. *OPTIMAL: Jurnal Ekonomi dan Manajemen, 4*(2), 223.

Safitri, Riska, J., Septi, S., Nining, N. E., Hutapea, D. N., & Nadiva , A. (2023). Strategi Inovasi Perbankan Digital dalam Menghadapi Persaingan Industri Keuangan . *Indonesian Journal of Economics, Management and Accounting, 1*(5), 417-418.

Sunarso, S. (2009). *Hukum Informasi dan Transaksi Elektronik* . Jakarta: Rineka Cipta.

T. , T., & U. , U. (2023). Perlindungan Hukum Terhadap Nasabah Bank Digital . *UNES Law Review, 6*(1), 1624-1635.

Tambunan, Ria, T., & M. Irwan Padli Nasution. (2023). Tantangan dan strategi perbankan dalam menghadapi perkembangan transformasi digitalisasi di era 4.0. *Sci-Tech Journal, 2*(2), 148-156.