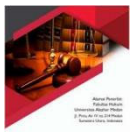
JURNAL NORMATIF
FAKULTAS HUKUM
UNIVERSITAS AL AZHAR



# CYBERCRIME PADA SISTEM PERBANKAN DIGITAL : EVALUASI KERENTANAN DAN UPAYA PERLINDUNGAN KONSUMEN

**Indra Gunawan Purba**

Program Pascasarjana llmu Hukum, Fakultas Hukum, Universitas Islam Smatera Utara Medan

Email : *1 indrapurba07081978@gmil.com

**Artikel Info**

**Artikel Historis** :

Terima: 4-12-2025

Terima dan di revisi: 6-12-2025

Disetujui: 11-12-2025

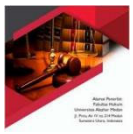
Kata Kunci : *Kejahatan Siber, Sistem Perbankan Digital, Perlindungan Konsumen*

**Abstrak**

kejahatan siber. Penelitian ini bertujuan untuk menganalisis bentuk dan karakteristik kerentanan dalam sistem perbankan digital, mengevaluasi efektivitas mekanisme perlindungan konsumen yang diterapkan oleh bank dan regulator, serta merumuskan langkah strategis untuk meningkatkan keamanan digital dalam merespons ancaman siber yang semakin canggih. Dengan menggunakan pendekatan kualitatif normatif–empiris, penelitian ini mengkaji regulasi, kebijakan industri, serta data empiris mengenai insiden kejahatan siber yang melibatkan layanan perbankan digital.

Temuan penelitian menunjukkan bahwa kerentanan dalam sistem perbankan digital bersifat multidimensional, mencakup aspek teknis, operasional, dan terkait pengguna. Meskipun mekanisme perlindungan konsumen oleh bank dan regulator telah diterapkan, efektivitasnya terkendala oleh ketidakmerataan penerapan standar keamanan, rendahnya literasi digital pengguna, serta cepatnya evolusi taktik kejahatan siber. Penelitian ini juga mengidentifikasi bahwa penguatan infrastruktur keamanan berbasis teknologi, harmonisasi pengawasan regulasi, dan peningkatan literasi keamanan digital merupakan strategi kunci untuk mewujudkan lingkungan perbankan digital yang aman dan berkelanjutan.

Secara keseluruhan, penelitian ini memberikan kontribusi terhadap pemahaman lebih mendalam mengenai kerentanan dan perlindungan konsumen dalam perbankan digital serta menawarkan rekomendasi strategis bagi bank, regulator, dan pemangku kepentingan untuk memperkuat ketahanan keamanan siber nasional



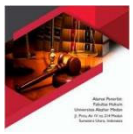
***Keywords:***
*Cybercrime, Digital Banking System, Consumer Protection*

***Abstract***

*The rapid development of digital technology has significantly transformed banking services but simultaneously increased exposure to cybercrime threats. This study aims to analyze the forms and characteristics of vulnerabilities in digital banking systems, evaluate the effectiveness of consumer protection mechanisms implemented by banks and regulators, and formulate strategic measures to enhance digital security in response to increasingly sophisticated cyber threats. Using a qualitative normative–empirical approach, the study examines regulations, industry policies, and empirical data on cybercrime incidents involving digital banking services.*

*The findings indicate that vulnerabilities in digital banking systems are multidimensional, encompassing technical, operational, and user-related aspects. While consumer protection mechanisms implemented by banks and regulators are in place, their effectiveness is hindered by uneven implementation of security standards, low digital literacy among users, and the rapid evolution of cybercrime tactics. The study also identifies that strengthening technology-based security infrastructure, harmonizing regulatory oversight, and enhancing digital security literacy are key strategies to establish a secure and sustainable digital banking environment.*

*Overall, this research contributes to a deeper understanding of vulnerabilities and consumer protection in digital banking and provides strategic recommendations for banks, regulators, and stakeholders to strengthen national cybersecurity resilience..*



## PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan pada industri perbankan, terutama melalui penerapan layanan perbankan digital yang memungkinkan transaksi dilakukan secara cepat, efisien, dan tanpa batas geografis. Transformasi ini meningkatkan kenyamanan nasabah sekaligus memperluas akses terhadap layanan keuangan. Namun, kemajuan tersebut juga menghadirkan risiko baru berupa meningkatnya ancaman kejahatan siber (cybercrime) yang secara langsung menyasar infrastruktur digital perbankan maupun pengguna akhir[1].

Kejahatan siber pada sektor perbankan berkembang dalam berbagai bentuk, mulai dari ***phishing, malware, SIM swap fraud, social engineering, ransomware***, hingga pencurian kredensial melalui teknik ***man-in-the-middle***. Motif dan modus pelaku semakin kompleks seiring berkembangnya teknologi, sehingga meningkatkan tingkat kerentanan sistem perbankan digital[2]. Di Indonesia, peningkatan laporan kejahatan digital pada sektor keuangan menunjukkan bahwa literasi digital masyarakat belum sebanding dengan tingkat penetrasi layanan digital perbankan.

Dampak kejahatan siber tidak hanya bersifat finansial, tetapi juga memengaruhi kepercayaan publik, stabilitas sistem keuangan, dan efektivitas regulasi yang dirancang untuk melindungi konsumen. Hal ini menempatkan bank dan regulator dalam posisi strategis untuk memperkuat tata kelola keamanan siber, meningkatkan kapabilitas deteksi ancaman, serta memastikan perlindungan konsumen berjalan secara optimal[3].

Dampak kejahatan siber dalam layanan perbankan digital tidak hanya bersifat finansial, tetapi juga menimbulkan konsekuensi yang lebih luas terhadap ekosistem keuangan secara keseluruhan. Secara finansial, serangan siber dapat menyebabkan kerugian langsung bagi nasabah maupun lembaga perbankan, baik melalui pencurian dana, manipulasi data, maupun penipuan transaksi elektronik. Namun, dampak yang paling signifikan seringkali terkait dengan kepercayaan publik. Ketika nasabah mengalami atau mendengar kasus kebocoran data atau transaksi yang terganggu akibat serangan siber, tingkat kepercayaan terhadap bank dan sistem pembayaran digital menurun, sehingga mengurangi adopsi teknologi finansial dan layanan digital.

Selain itu, kejahatan siber juga berpotensi mengganggu stabilitas sistem keuangan. Serangan berskala besar, seperti malware atau ransomware yang menargetkan infrastruktur perbankan, dapat menghambat operasi transaksi, memicu kepanikan di pasar, dan meningkatkan risiko sistemik bagi seluruh industri keuangan. Hal ini menunjukkan bahwa keamanan siber tidak hanya menjadi tanggung jawab setiap bank, tetapi juga menjadi isu strategis bagi regulator dan pemerintah.

Dampak lain yang tidak kalah penting adalah pada efektivitas regulasi yang dirancang untuk melindungi konsumen. Ketika serangan siber berhasil mengeksploitasi celah sistem atau prosedur bank, maka peraturan yang ada bisa menjadi kurang efektif dalam memberikan perlindungan. Hal ini menuntut lembaga keuangan dan regulator untuk terus memperbarui kebijakan, meningkatkan pemantauan, dan mengadopsi teknologi baru untuk menyesuaikan diri dengan ancaman yang terus berkembang. Dengan kata lain, kejahatan siber menekankan perlunya pendekatan keamanan yang holistik dan adaptif, di mana teknologi, regulasi, dan edukasi konsumen berjalan secara terpadu untuk menjaga stabilitas, kepercayaan, dan perlindungan finansial

Oleh karena itu, penelitian mengenai evaluasi kerentanan sistem perbankan digital dan upaya perlindungan konsumen menjadi semakin penting. Analisis komprehensif diperlukan untuk mengidentifikasi titik lemah yang masih terbuka, menilai efektivitas kebijakan yang telah diterapkan, serta memberikan rekomendasi strategis guna meminimalkan risiko kejahatan siber di sektor perbankan.

Berdasarkan latar belakang tersebut perlu dikaji permasalahan sebagai berikut:

1. Bagaimana bentuk dan karakteristik kerentanan (vulnerabilities) dalam sistem

[1] **Bank for International Settlements.** "Cybersecurity in Banking," *BIS Working Papers*, 2020, hlm. 45

[2] **European Union Agency for Cybersecurity (ENISA).** *Threat Landscape Report*, 2022, hlm.35

[3] **Otoritas Jasa Keuangan (OJK).** *Perlindungan Konsumen Sektor Jasa Keuangan dalam Era Digital*, OJK Research Publication, 2023, hlm.6

perbankan digital yang berpotensi dieksploitasi oleh pelaku cybercrime di era perkembangan teknologi saat ini?
2. Sejauh mana efektivitas mekanisme perlindungan konsumen dalam mencegah, mendeteksi, dan menangani kasus kejahatan siber pada layanan perbankan digital?
3. Upaya strategis apa saja yang perlu diperkuat atau dikembangkan untuk meningkatkan keamanan sistem perbankan digital dan memastikan perlindungan konsumen yang optimal terhadap ancaman kejahatan siber yang semakin kompleks?

## METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan model normatif–empiris. Pendekatan normatif digunakan untuk menganalisis kerangka hukum, regulasi, standar keamanan perbankan digital, serta pengaturan perlindungan konsumen dalam konteks kejahatan siber. Pendekatan empiris digunakan untuk memahami praktik di lapangan melalui data aktual terkait kasus cybercrime, mekanisme penanganan, dan implementasi kebijakan pada industri perbankan digital.

Pendekatan ini memungkinkan analisis komprehensif antara teks norma dan realitas penerapannya.

## HASIL DAN PEMBAHASAN.

### Bentuk dan Karakteristik Kerentanan dalam Sistem Perbankan Digital

Perkembangan teknologi digital dalam sektor perbankan telah mendorong inovasi layanan keuangan secara masif. Namun digitalisasi ini sekaligus membuka celah kerentanan (*vulnerabilities*) yang dapat dieksploitasi oleh pelaku cybercrime. Kerentanan tersebut dapat dikategorikan ke dalam tiga dimensi utama : **kerentanan teknis, kerentanan operasional,** dan **kerentanan berbasis perilaku konsumen**.

Perkembangan teknologi digital telah mendorong transformasi besar dalam industri perbankan. Digitalisasi memungkinkan lembaga keuangan menghadirkan layanan yang lebih cepat, efisien, dan berorientasi pada pengalaman pengguna. Salah satu perubahan paling signifikan adalah pergeseran dari layanan konvensional di kantor cabang menuju layanan berbasis mobile dan internet. Nasabah kini dapat mengakses layanan kapan saja dan di mana saja, mulai dari cek saldo hingga transaksi investasi[4]

Inovasi seperti mobile banking, internet banking, dan pembayaran berbasis QR telah mempercepat proses transaksi serta memperkuat keamanan melalui autentikasi berlapis seperti biometrik dan OTP. Integrasi kecerdasan buatan (AI) dan machine learning memungkinkan bank menganalisis pola transaksi pengguna, mendeteksi potensi kecurangan (fraud), dan memberikan rekomendasi finansial secara personal[5]. Teknologi ini juga mendukung otomasi pengambilan keputusan dalam berbagai aktivitas operasional perbankan[6].

Selain itu, munculnya bank digital (*digital-only bank*) mengubah model bisnis perbankan tradisional. Bank digital beroperasi tanpa kantor fisik dan mengandalkan aplikasi sebagai kanal utama layanan. Efisiensi biaya operasional memungkinkan bank digital menawarkan suku bunga lebih menarik, membuka rekening lebih cepat, dan memberikan layanan mandiri yang lebih mudah diakses[7].

Perkembangan open banking dan penggunaan Application Programming Interface (API) membuka peluang kolaborasi antara bank dan perusahaan *financial technology* (fintech). Pola ini menciptakan ekosistem keuangan yang lebih terbuka, inovatif, dan kompetitif[8]. Sementara itu, teknologi blockchain memberi terobosan dalam pencatatan transaksi yang transparan, aman, dan sulit dimanipulasi, sehingga berpotensi meningkatkan keamanan sistem pembayaran dan transfer lintas negara[9].

Secara keseluruhan, digitalisasi mendorong efisiensi operasional bank, pemerataan akses keuangan, serta peningkatan keamanan transaksi. Meski demikian, perkembangan ini perlu diimbangi

[4] Kasmir, *Bank dan Lembaga Keuangan Lainnya*, Edisi Revisi, 2014, hlm. 161

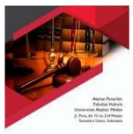
[5] Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Humans*, 2019, hlm. 178

[6] John Hull, *Risk Management and Financial Institutions*, 5th ed., 2018, hlm. 412

[7] Jogiyanto HM, *Sistem Informasi Manajemen*, Edisi Revisi, 2005, hlm. 35

[8] Chris Skinner, *Digital Bank: Strategies to Launch or Become a Digital Bank*, 2014, hlm. 29

[9] Don Tapscott & Alex Tapscott, *Blockchain Revolution*, 2016, hlm. 25



dengan regulasi yang kuat dan edukasi masyarakat agar risiko keamanan siber dapat diminimalkan[10].

Pertama, **kerentanan teknis** (*technical vulnerabilities*) terjadi ketika sistem tidak sepenuhnya terlindungi oleh mekanisme keamanan berlapis. Contohnya adalah kelemahan pada autentikasi pengguna, penggunaan enkripsi yang tidak mutakhir, celah pada aplikasi mobile banking, serta kurang optimalnya perlindungan terhadap serangan *man-in-the-middle*, *malware*, dan *credential theft*. Serangan siber yang memanfaatkan *zero-day vulnerabilities* menjadi ancaman signifikan karena memanfaatkan celah yang belum terdeteksi oleh penyedia layanan perbankan.

Kedua, **kerentanan operasional** (*operational vulnerabilities*) muncul akibat kelemahan dalam tata kelola keamanan internal perbankan. Ini dapat terjadi pada proses verifikasi data, monitoring transaksi, serta kurangnya integrasi sistem pencegahan fraud. Keterlambatan dalam mendeteksi anomali transaksi, lemahnya segmentasi jaringan, atau inkonsistensi kebijakan keamanan antar-unit membuat bank semakin rentan terhadap serangan siber yang bersifat terorganisir.

Ketiga, **kerentanan berbasis perilaku konsumen** (*human-related vulnerabilities*) merupakan faktor dominan dalam banyak kasus *cybercrime*. Rendahnya literasi digital menyebabkan konsumen mudah terjebak dalam rekayasa sosial (*phishing*, *vishing*, *smishing*), penyalahgunaan OTP, atau tautan palsu yang menyerupai aplikasi resmi perbankan. Pelaku *cybercrime* memanfaatkan manipulasi psikologis untuk meraih akses tanpa harus menyerang sistem teknologi secara langsung.

Dari analisis ini dapat disimpulkan bahwa kerentanan pada sistem perbankan digital bersifat **multidimensional**, sehingga penanggulangannya membutuhkan pendekatan yang komprehensif antara aspek teknologi, operasional, dan edukasi konsumen.

**Efektivitas Mekanisme Perlindungan Konsumen dalam Menghadapi Kejahatan Siber**

Upaya perlindungan konsumen dalam layanan perbankan digital diselenggarakan melalui kombinasi pendekatan teknis, regulatif, dan prosedural. Namun, efektivitasnya masih menghadapi tantangan seiring meningkatnya kompleksitas serangan siber. Dari sisi perbankan, berbagai mekanisme telah diterapkan seperti autentikasi multifaktor (MFA), enkripsi data, sistem deteksi anomali, teknologi biometrik, serta *real-time monitoring*. Meskipun demikian, efektivitasnya sangat bergantung pada konsistensi implementasi dan kemampuan setiap bank dalam memperbarui sistem keamanan. Beberapa bank dengan infrastruktur yang lebih maju menunjukkan tingkat pencegahan serangan yang lebih baik dibandingkan institusi yang masih berada pada tahap awal transformasi digital. Perlindungan konsumen dalam layanan perbankan digital menjadi sangat krusial seiring dengan meningkatnya adopsi teknologi informasi di sektor keuangan. Upaya perlindungan ini dilaksanakan melalui kombinasi pendekatan teknis, regulatif, dan prosedural yang saling melengkapi untuk menjaga keamanan, kepercayaan, dan hak-hak nasabah[11]. Pendekatan teknis berfokus pada penerapan teknologi keamanan siber yang mampu melindungi data dan transaksi nasabah dari ancaman yang semakin kompleks. Bank dan penyedia layanan keuangan memanfaatkan autentikasi berlapis, seperti penggunaan OTP, biometrik, dan token digital, serta enkripsi data end-to-end agar informasi tetap aman selama proses transmisi[12]. Selain itu, sistem deteksi dan pencegahan intrusi digunakan untuk memantau aktivitas mencurigakan dan merespons ancaman secara real-time. Integrasi kecerdasan buatan (AI) memungkinkan analisis pola transaksi

[10] Erik Brynjolfsson & Andrew McAfee, *The Second Machine Age*, 2014, hlm. 105

[11] Kasmir, *Bank dan Lembaga ... Op.Cit.* hlm. 170

[12] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., 2021, hlm. 23

secara otomatis, membantu mendeteksi potensi kecurangan, serta memberikan rekomendasi personal bagi nasabah[13].

Pendekatan regulatif menjadi fondasi hukum bagi perlindungan konsumen. Bank dan penyedia layanan digital diwajibkan mematuhi aturan yang ditetapkan oleh otoritas keuangan, seperti Peraturan Bank Indonesia tentang layanan perbankan digital dan Peraturan OJK mengenai perlindungan konsumen dan literasi keuangan[14]. Regulasi ini menetapkan standar keamanan transaksi elektronik, hak-hak nasabah, kewajiban edukasi, serta prosedur penyelesaian sengketa, sehingga lembaga keuangan memiliki tanggung jawab hukum atas kerugian yang mungkin dialami nasabah akibat kesalahan teknis atau serangan siber.

Selain itu, pendekatan prosedural menekankan pentingnya proses internal bank dalam melindungi konsumen. Prosedur ini mencakup edukasi dan sosialisasi literasi digital kepada nasabah, sehingga mereka memahami risiko yang mungkin muncul dan dapat melindungi akun mereka secara mandiri[15]. Bank juga diwajibkan menyediakan mekanisme penanganan keluhan dan sengketa yang cepat dan transparan, serta melakukan audit internal dan penilaian risiko secara berkala. Langkah-langkah ini membantu meminimalkan risiko human error dan meningkatkan kesadaran nasabah terhadap potensi ancaman siber[16].

Meskipun kombinasi pendekatan teknis, regulatif, dan prosedural telah diterapkan, efektivitas perlindungan konsumen masih menghadapi tantangan seiring meningkatnya kompleksitas serangan siber, seperti phishing, malware, dan ransomware. Perkembangan teknologi yang cepat juga menuntut sistem keamanan untuk selalu diperbarui agar tetap efektif. Selain itu, literasi digital nasabah yang bervariasi membuat sebagian pengguna masih rentan terhadap penipuan atau kesalahan penggunaan layanan digital[17]. Oleh karena itu, perlindungan konsumen dalam perbankan digital memerlukan strategi yang berlapis dan adaptif, mencakup inovasi teknologi, regulasi yang responsif, dan edukasi berkelanjutan bagi nasabah serta tenaga profesional perbankan.

Dari sisi regulator, Otoritas Jasa Keuangan (OJK) dan Bank Indonesia telah menetapkan standar keamanan minimum, pedoman manajemen risiko TI, dan mekanisme perlindungan konsumen melalui regulasi, pengawasan, serta penanganan pengaduan. Namun terdapat kendala dalam harmonisasi pengawasan, khususnya terkait penerapan standar keamanan antara bank besar dan bank kecil, serta kesiapan pelaksanaan audit keamanan secara berkala.

Sementara itu, efektivitas perlindungan konsumen dari perspektif pengguna cenderung bergantung pada tingkat literasi digital. Program edukasi publik terkait ancaman siber masih jauh dari optimal, sehingga konsumen sering kali tidak menyadari risiko penggunaan perangkat pribadi yang tidak aman, pengunduhan aplikasi palsu, atau pembocoran data pribadi melalui media sosial.

Secara keseluruhan, mekanisme perlindungan konsumen telah berjalan namun

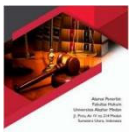
[13] John Hull, *Risk Management …Op.Cit*, hlm. 420

[14] Bank Indonesia, *Peraturan Bank Indonesia tentang Layanan Perbankan Digital*, 2020

[15] Jogiyanto HM, *Sistem Informasi…..Op.Cit*, hlm. 42

[16] Chris Skinner, *Digital Bank: Strategies to Launch or Become a Digital Bank*, 2014, hlm. 158

[17] Erik Brynjolfsson & Andrew McAfee, *The Second Machine Age*, 2014, hlm. 140



belum sepenuhnya efektif. Ketimpangan implementasi standar keamanan, keterbatasan literasi konsumen, dan kecepatan evolusi modus kejahatan siber membuat perlindungan yang ada masih bersifat **reaktif** dan belum mampu memastikan pencegahan secara menyeluruh.

**Upaya Strategis untuk Meningkatkan Keamanan Sistem Perbankan Digital dan Perlindungan Konsumen**

Untuk menjawab tantangan cybercrime yang semakin kompleks, diperlukan strategi penguatan keamanan dan perlindungan konsumen secara lebih terarah, terukur, dan adaptif. Upaya strategis tersebut dapat dikategorikan dalam tiga arah kebijakan : **penguatan infrastruktur keamanan, penguatan regulasi dan koordinasi pengawasan**, dan **pemberdayaan konsumen**.

Pertama, penguatan infrastruktur keamanan harus mencakup penerapan *advanced threat detection*, teknologi kecerdasan buatan (AI) untuk analisis pola anomali, serta penguatan *zero trust architecture*. Bank juga perlu memperkuat keamanan API dan integrasi sistem mengingat ekspansi menuju *open banking* yang membuka peluang serangan lintas platform.

Menghadapi tantangan cybercrime yang semakin kompleks, sektor perbankan digital memerlukan strategi penguatan keamanan dan perlindungan konsumen yang bersifat terarah, terukur, dan adaptif. Strategi ini harus mengintegrasikan inovasi teknologi, kebijakan regulatif, serta prosedur internal yang konsisten, agar mampu mengantisipasi berbagai ancaman siber, mulai dari phishing, malware, hingga serangan *ransomware*.

Penguatan keamanan secara terarah mencakup penerapan teknologi canggih seperti autentikasi *multi-lapis, enkripsi data end-to-end*, dan sistem deteksi intrusi berbasis kecerdasan buatan (AI) yang dapat memantau pola transaksi dan mendeteksi aktivitas mencurigakan secara real-time[18]. Dengan pendekatan ini, bank tidak hanya melindungi data dan aset nasabah, tetapi juga membangun kepercayaan terhadap layanan digital yang disediakan.

Keamanan yang **terukur** memerlukan evaluasi risiko dan audit berkala terhadap sistem dan prosedur internal bank. Hal ini mencakup pemantauan kerentanan, penilaian efektivitas kontrol keamanan, dan pelaporan insiden secara sistematis[19]. Dengan pengukuran yang jelas, lembaga keuangan dapat menentukan prioritas mitigasi risiko serta mengalokasikan sumber daya secara efisien, sehingga perlindungan konsumen dapat berjalan optimal tanpa menimbulkan beban operasional yang berlebihan.

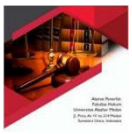
Sementara itu, pendekatan adaptif menuntut institusi keuangan untuk terus menyesuaikan strategi keamanan dengan perkembangan teknologi dan pola serangan siber yang dinamis. Regulasi dan prosedur internal harus fleksibel, mampu merespons perubahan lingkungan digital, dan didukung literasi digital bagi nasabah agar mereka paham risiko serta cara melindungi diri dari potensi penipuan[20]. Strategi adaptif ini memungkinkan bank dan fintech untuk menjaga keberlanjutan layanan digital sekaligus meminimalkan risiko bagi konsumen.

Dengan kombinasi strategi yang terarah, terukur, dan adaptif, perlindungan konsumen dalam layanan perbankan digital tidak hanya menjadi respons terhadap ancaman siber, tetapi juga menjadi bagian integral dari manajemen risiko dan inovasi layanan keuangan modern[21]. Upaya ini menekankan bahwa keamanan dan perlindungan konsumen harus selalu menjadi prioritas utama dalam ekosistem perbankan digital yang terus berkembang.

Kedua, dari sisi regulatif, diperlukan harmonisasi standar keamanan antara regulator, bank, dan penyelenggara teknologi keuangan. Penguatan audit dan sertifikasi keamanan TI secara berkala sangat penting untuk memastikan kepatuhan. Regulasi juga perlu diperbarui secara dinamis agar responsif terhadap teknologi baru dan pola kejahatan yang berkembang.

Ketiga, pemberdayaan konsumen harus dilakukan melalui edukasi digital yang berkesinambungan. Pelatihan keamanan siber berbasis kampanye publik, pemberian peringatan real-time melalui aplikasi perbankan, dan peningkatan transparansi risiko perlu menjadi

[18] Melanie Mitchell, *Artificial Intelligence: .... Op.Cit,* hlm. 178
[19] John Hull, *Risk Management ..... Op, Cit*, hlm. 412
[20] Otoritas Jasa Keuangan, *Peraturan OJK tentang Perlindungan Konsumen dan Literasi Keuangan*, 2018
[21] Chris Skinner, *Digital Bank…… Op.Cit*, hlm. 145–158



prioritas. Konsumen yang lebih sadar risiko cenderung mampu menolak dan melaporkan upaya penipuan sejak awal.

Dengan demikian, upaya strategis yang terintegrasi antara teknologi, regulasi, dan edukasi konsumen akan memperkuat ketahanan sistem perbankan digital sekaligus meningkatkan perlindungan konsumen terhadap ancaman kejahatan siber yang semakin canggih.

.

## PENUTUP

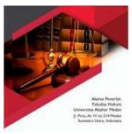
### Kesimpulan

Berdasarkan hasil analisis mengenai kerentanan, efektivitas perlindungan konsumen, dan upaya strategis dalam menghadapi kejahatan siber pada sistem perbankan digital, dapat disimpulkan beberapa hal sebagai berikut:

1. **Kerentanan dalam sistem perbankan digital bersifat multidimensional**, mencakup aspek teknis, operasional, dan perilaku konsumen. Kerentanan teknis muncul melalui celah keamanan aplikasi, enkripsi yang tidak mutakhir, dan serangan seperti phishing, malware, atau *man-in-the-middle*. Kerentanan operasional dipengaruhi oleh lemahnya tata kelola keamanan internal, sedangkan kerentanan berbasis perilaku konsumen muncul akibat rendahnya literasi digital dan tingginya keberhasilan rekayasa sosial.
2. **Efektivitas mekanisme perlindungan konsumen masih menghadapi sejumlah tantangan.** Meskipun perbankan telah menerapkan autentikasi berlapis, enkripsi, sistem deteksi anomali, dan pengawasan berkelanjutan, implementasinya belum merata antar-institusi. Regulator juga telah mengatur standar keamanan dan mekanisme perlindungan konsumen, namun harmonisasi kebijakan serta tingkat kepatuhan bank masih perlu diperkuat. Di sisi lain, peran konsumen masih menjadi titik lemah utama karena rendahnya kesadaran terhadap ancaman siber.
3. **Upaya strategis yang diperlukan dalam menghadapi kejahatan siber bersifat integratif**, mencakup penguatan infrastruktur keamanan berbasis teknologi mutakhir, penegasan standar regulasi dan pengawasan yang responsif terhadap perkembangan teknologi, serta pemberdayaan konsumen melalui edukasi digital yang berkelanjutan. Sinergi antara bank, regulator, dan konsumen merupakan syarat utama bagi terciptanya sistem perbankan digital yang lebih aman, adaptif, dan berkelanjutan.

### Saran

1. **Penguatan Keamanan Teknologi Perbankan** Perbankan perlu memperbarui arsitektur keamanannya melalui penerapan *zero-trust security*, *advanced threat intelligence*, serta pemanfaatan teknologi kecerdasan buatan (AI) dan *machine learning* dalam mendeteksi anomali transaksi secara real-time. Audit keamanan siber harus dilakukan secara berkala untuk memastikan bahwa celah teknologi dapat diminimalkan.
2. **Optimalisasi Peran Regulator dan Harmonisasi Kebijakan** Regulator perlu memperkuat harmonisasi standar keamanan antar-bank, memperketat pengawasan implementasi manajemen risiko TI, serta memperbarui kebijakan secara adaptif mengikuti dinamika modus kejahatan siber. Koordinasi antara OJK, BI, dan lembaga keamanan siber nasional perlu ditingkatkan untuk menciptakan ekosistem pengawasan yang lebih terpadu.
3. **Pemberdayaan Konsumen melalui Literasi Keamanan Digital,** Program edukasi publik mengenai keamanan digital harus dilakukan secara intensif dan berkelanjutan. Bank perlu menyediakan notifikasi real-time mengenai potensi ancaman, panduan keamanan yang mudah diakses, serta kampanye anti-phishing yang terintegrasi di aplikasi mereka. Pemberdayaan konsumen merupakan komponen penting untuk menekan keberhasilan serangan berbasis rekayasa sosial.
4. **Peningkatan Transparansi dan Mekanisme Penanganan Pengaduan** Bank perlu meningkatkan transparansi terkait risiko siber dan mempercepat proses penanganan pengaduan nasabah yang menjadi korban. Mekanisme kompensasi, pemulihan akun, dan investigasi insiden harus dilakukan lebih cepat, konsisten, dan akuntabel untuk menjaga kepercayaan publik.
5. **Kolaborasi Multi-Pihak** Kerja sama antara industri perbankan, regulator, penyelenggara fintech, dan lembaga akademik perlu ditingkatkan untuk menciptakan basis pengetahuan bersama, berbagi data insiden, serta menyusun protokol respons siber yang lebih komprehensif.



**DAFTAR PUSTAKA**

Chris Skinner, *Digital Bank: Strategies to Launch or Become a Digital Bank*, 2014.

Don Tapscott & Alex Tapscott, *Blockchain Revolution*, 2016.

Erik Brynjolfsson & Andrew McAfee, *The Second Machine Age*, 2014.

**European Union Agency for Cybersecurity (ENISA).** *Threat Landscape Report*, 2022

Erik Brynjolfsson & Andrew McAfee, *The Second Machine Age*, 2014.

Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Humans*, 2019

John Hull, *Risk Management and Financial Institutions*, 5th ed., 2018

Jogiyanto HM, *Sistem Informasi Manajemen*, Edisi Revisi, 2005.

Kasmir, *Bank dan Lembaga Keuangan Lainnya*, Edisi Revisi, 2014

Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., 2021.

Peraturan Perundang-udangan :

Bank Indonesia, *Peraturan Bank Indonesia tentang Layanan Perbankan Digital*, 2020

**Bank for International Settlements.** "Cybersecurity in Banking," *BIS Working Papers*, 2020.

**Otoritas Jasa Keuangan (OJK).** *Perlindungan Konsumen Sektor Jasa Keuangan dalam Era Digital*, OJK Research Publication, 2023

Otoritas Jasa Keuangan, *Peraturan OJK tentang Perlindungan Konsumen dan Literasi Keuangan*, 2018