aml/cft journal
journal of anti-money laundering / countering the financing of terrorism

Original paper

Evolusi dan Pola Kejahatan dalam Sistem Perbankan: Dari Penipuan Tradisional hingga Kejahatan Siber

Mohamad Nur Efendi[1*], Mukhtar Adinugroho[2], Selvina Khomairoh[3]
[1] Fakultas Ekonomi dan Bisnis, Universitas Terbuka, Indonesia
[2] Fakultas Ekonomi Bisnis dan Teknologi Digital, Universitas Nahdlatul Ulama Surabaya, Indonesia
[3] Departemen Administrasi Bisnis Sains, Universitas Terbuka, Indonesia

Korespondensi penulis: md.nur.efendi@gmail.com

Kata Kunci:
Evolusi Kejahatan Perbankan, Keamanan Perbankan, Kejahatan Siber, Penipuan Tradisional, Tren Penipuan Digital

Abstrak

Studi ini membahas perubahan pola kejahatan di sektor perbankan, yang kini bergeser dari penipuan konvensional ke bentuk kejahatan siber yang lebih kompleks seperti phishing, ransomware, dan pembobolan data. Perkembangan teknologi, khususnya digitalisasi dan inovasi keuangan, telah mengubah cara kerja pelaku kejahatan yang kini memanfaatkan celah sistem digital, sehingga menimbulkan tantangan baru dalam pengelolaan risiko keamanan oleh institusi perbankan. Menggunakan metode studi pustaka, penelitian ini mengkaji literatur akademik dan praktik industri terkini terkait kejahatan siber serta Tindak Pidana Pencucian Uang (TPPU) dan Pendanaan Terorisme (TPPT). Kejahatan siber sering dimanfaatkan untuk memfasilitasi pencucian uang dan pendanaan terorisme melalui transaksi lintas negara yang sulit ditelusuri. Rekomendasi utama mencakup pemanfaatan teknologi canggih seperti sistem deteksi anomali berbasis kecerdasan buatan (AI), penguatan regulasi keamanan siber perbankan, serta peningkatan edukasi bagi pegawai dan nasabah. Selain itu, studi ini mendorong peningkatan kapasitas PPATK dalam mengawasi transaksi digital dan memperkuat kerja sama internasional dalam pertukaran informasi terkait TPPU dan TPPT. Kolaborasi antar sektor, termasuk lembaga keuangan, otoritas pengawas, dan penyedia teknologi, dinilai penting untuk memperkuat ketahanan sistem keuangan serta mendukung efektivitas rezim APU PPT di Indonesia di tengah tantangan era digital.

Dikirimkan: 1 Agustus 2024
Diterima: 14 Mei 2025
Diterbitkan: 27 Juni 2025

***Untuk mensitasi artikel ini*:** Efendi, M. N., Adinugroho, M & Khomairoh, S. 2025. *Evolusi dan Pola Kejahatan dalam Sistem Perbankan: Dari Penipuan Tradisional hingga Kejahatan Siber. AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 3(2):168-196, https://doi.org/10.59593/amlcft.2025.v3i2.219

Pendahuluan

Kejahatan dalam sistem perbankan telah mengalami evolusi yang signifikan seiring dengan perkembangan teknologi dan digitalisasi.[1] Di masa lalu, kejahatan perbankan umumnya berbentuk penipuan tradisional, seperti pemalsuan cek, penggelapan dana, dan pencurian

[1] Monica Violeta Achim and Sorin Nicolae Borlea, *Economic and Financial Crime: Corruption, Shadow Economy, and Money Laundering*, vol. 20, Studies of Organized Crime (Cham: Springer International Publishing, 2020), https://doi.org/10.1007/978-3-030-51780-9.

identitas melalui dokumen fisik.[2] Teori-teori kriminologi tradisional, seperti teori pilihan rasional, berasumsi bahwa pelaku kejahatan melakukan tindak kriminal setelah mempertimbangkan risiko dan manfaat yang mungkin diperoleh.[3] Dalam konteks perbankan, pelaku biasanya memanfaatkan kelemahan dalam sistem keamanan yang ada, seperti kurangnya pengawasan internal atau ketidakkonsistenan dalam prosedur operasional.[4] Model pengendalian penipuan tradisional menekankan pentingnya pengawasan internal, audit berkala, serta verifikasi identitas yang ketat sebagai upaya untuk mencegah dan mendeteksi tindak kejahatan.[5]

Munculnya era digital telah menyebabkan pola kejahatan dalam dunia perbankan bergeser ke arah kejahatan siber, yang mencakup berbagai bentuk kejahatan seperti *phishing*, *malware, ransomware*, dan peretasan sistem.[6] Teori-teori baru dalam kriminologi siber, seperti teori rutinitas aktivitas dan teori netralisasi, dikembangkan untuk menjelaskan fenomena ini. Menurut teori rutinitas aktivitas, peluang terjadinya kejahatan meningkat ketika terdapat target yang rentan, pelaku yang termotivasi, dan tidak adanya pengawas.[7] Dalam konteks digital, kemudahan akses terhadap informasi dan data, ditambah dengan lemahnya sistem keamanan, menciptakan lingkungan yang ideal bagi pelaku kejahatan siber. Selain itu, teori netralisasi menjelaskan bahwa pelaku kejahatan siber sering membenarkan tindakan mereka dengan meremehkan atau menyangkal dampak negatif yang ditimbulkan.[8] Pergeseran ini menunjukkan bahwa para pelaku kejahatan semakin mengadopsi teknologi canggih untuk mengeksploitasi kerentanan dalam sistem perbankan digital, sehingga dibutuhkan pendekatan baru dalam pengendalian kejahatan yang lebih adaptif dan inovatif.

Studi mengenai evolusi kejahatan dalam sistem perbankan telah menarik perhatian para peneliti, dengan fokus yang semakin besar terhadap pergeseran dari penipuan tradisional ke kejahatan siber. Choi dkk. (2017) menyoroti bahwa kejahatan tradisional seperti pencurian identitas dan pemalsuan cek telah mengalami penurunan seiring dengan meningkatnya keamanan fisik dan penerapan regulasi yang lebih ketat dalam sistem perbankan.[9] Laporan dari Hasham dkk. (2019) menunjukkan peningkatan pesat dalam kejahatan siber, khususnya dalam bentuk serangan phishing dan ransomware, yang menjadi ancaman serius terhadap integritas sistem perbankan digital.[10] Studi yang dilakukan oleh Lokanan juga membahas bagaimana perkembangan teknologi, seperti penggunaan layanan perbankan berbasis internet, telah

[2] Mark Lokanan, "Theorizing Financial Crimes as Moral Actions," *European Accounting Review* 27, no. 5 (2018): 901–38, https://doi.org/10.1080/09638180.2017.1417144.

[3] Shazeeda Ali, "Criminal Minds: Profiling Architects of Financial Crimes," *Journal of Financial Crime* 28, no. 2 (2021): 324–44, https://doi.org/10.1108/JFC-11-2020-0221.

[4] Hafiza Aishah Hashim et al., "The Risk of Financial Fraud: A Management Perspective," *Journal of Financial Crime* 27, no. 4 (2020): 1143–59, https://doi.org/10.1108/JFC-04-2020-0062.

[5] Nancy Reichman, "Managing Crime Risks: Toward an Insurance Based Model of Social Control," in *Risk Management*, ed. Gerald Mars and David T. H. Weir (London: Routledge, 2020), 45–66.

[6] Yoga Pratama et al., "Cybercrime: The Phenomenon of Crime through the Internet in Indonesia," *Proceeding International Conference Restructuring and Transforming Law* 1, no. 1 (2022): 294–301.

[7] Brian K. Payne, "Defining Cybercrime," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, ed. Thomas J. Holt and Adam M. Bossler (Cham: Palgrave Macmillan, 2020), 3–25, https://doi.org/10.1007/978-3-319-78440-3_1.

[8] Mochammad Fahlevi et al., "Cybercrime Business Digital in Indonesia," *E3S Web of Conferences* 125 (2019): 21001, https://doi.org/10.1051/e3sconf/201912521001.

[9] Kwan Choi, Ju-lak Lee, and Yong-tae Chun, "Voice Phishing Fraud and Its Modus Operandi," *Security Journal* 30, no. 2 (2017): 454–66, https://doi.org/10.1057/sj.2014.49.

[10] Salim Hasham, Shoan Joshi, and Daniel Mikkelsen, *Financial Crime and Fraud in the Age of Cybersecurity* (New Yok: McKinsey & Company, 2019).

menciptakan peluang baru bagi pelaku kejahatan siber untuk mengeksploitasi celah keamanan yang ada.[11]

Modus operandi umumnya merujuk pada metode khas atau pola perilaku yang secara konsisten digunakan oleh seseorang, terutama pelaku kejahatan, dalam melakukan tindakan melawan hukum. Dalam konteks kejahatan siber, *modus operandi* mencakup teknik, strategi, dan alat tertentu yang digunakan oleh pelaku untuk mengeksploitasi kerentanan dalam sistem digital. Pospisil dkk. (2020) menekankan pentingnya pemahaman mendalam terhadap *modus operandi* kejahatan siber dalam merumuskan strategi pencegahan yang efektif.[12] Studi ini sejalan dengan temuan Reichman yang menunjukkan bahwa teknik *social engineering* telah menjadi alat utama bagi pelaku kejahatan untuk menipu individu dan mengakses data sensitif.[13] Van Nguyen meneliti bagaimana jaringan kejahatan transnasional sering kali menjadi pelaku kejahatan siber, yang menunjukkan kompleksitas dan skala global dari permasalahan ini.[14] Sementara itu, studi oleh Trozze dkk. (2022) menambahkan bahwa kemunculan mata uang kripto telah memperkenalkan dimensi baru dalam kejahatan perbankan, di mana transaksi yang sulit dilacak memberikan keuntungan bagi para pelaku kejahatan.[15]

Banyak studi telah mengkaji berbagai aspek kejahatan perbankan, namun masih terdapat kesenjangan dalam pemahaman mengenai dampak transformasi teknologi terhadap pola kejahatan serta respons perbankan. Beberapa penelitian, seperti yang dilakukan oleh Jakšič dan Marinč, telah menyoroti peran kecerdasan buatan dan teknologi finansial dalam memitigasi kejahatan siber, namun masih terbatas dalam mengaitkan evolusi dari penipuan tradisional menuju kejahatan siber secara komprehensif.[16] Kesenjangan ini mencakup pemahaman tentang bagaimana pola kejahatan perbankan yang semakin kompleks berpotensi dimanfaatkan sebagai sarana Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT), seiring dengan berkembangnya teknik-teknik yang digunakan untuk menyamarkan asal-usul dana ilegal. Penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan menganalisis secara komprehensif evolusi tipologi kejahatan perbankan dan dampaknya terhadap kebijakan pencegahan tindak pidana di era digital. Dengan memetakan transformasi pola kejahatan serta mengevaluasi efektivitas kebijakan keamanan yang telah ada, diharapkan dapat diidentifikasi langkah-langkah pencegahan yang lebih adaptif dalam menghadapi risiko TPPU dan TPPT di masa mendatang.

Penelitian ini menggunakan metode tinjauan pustaka untuk menganalisis evolusi pola kejahatan dalam sistem perbankan, dengan fokus pada bagaimana digitalisasi dan teknologi finansial memengaruhi *modus operandi* pelaku dalam Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT). Literatur yang dikaji dipilih berdasarkan publikasi dari tahun 2017 hingga 2024, dengan penekanan pada artikel yang telah melalui proses *peer review,* laporan regulasi, dan makalah kebijakan di bidang kriminologi, keamanan siber, anti-pencucian uang, serta kebijakan perbankan. Sumber-sumber literatur diidentifikasi melalui basis data seperti Scopus, ScienceDirect, JSTOR, dan Google Scholar dengan

[11] Lokanan, "Theorizing Financial Crimes as Moral Actions."

[12] Bettina Pospisil et al., "Modus Operandi in Cybercrime," in *Encyclopedia of Criminal Activities and the Deep Web* (IGI Global Scientific Publishing, 2020), 193–209, https://doi.org/10.4018/978-1-5225-9715-5.ch013.

[13] Reichman, "Managing Crime Risks."

[14] Trong Van Nguyen, "The Modus Operandi of Transnational Computer Fraud: A Crime Script Analysis in Vietnam," *Trends in Organized Crime* 25, no. 2 (2022): 226–47, https://doi.org/10.1007/s12117-021-09422-1.

[15] Arianna Trozze et al., "Cryptocurrencies and Future Financial Crime," *Crime Science* 11, no. 1 (2022): 1, https://doi.org/10.1186/s40163-021-00163-8.

[16] Marko Jakšič and Matej Marinč, "Relationship Banking and Information Technology: The Role of Artificial Intelligence and FinTech," *Risk Management* 21, no. 1 (2019): 1–18, https://doi.org/10.1057/s41283-018-0039-y.

menggunakan kata kunci yang relevan. Studi yang dipilih secara khusus membahas kejahatan keuangan berbasis siber, peran platform digital dalam menyembunyikan dana ilegal, serta respons regulatif, sehingga memungkinkan peneliti untuk memberikan rekomendasi yang terinformasi dalam upaya peningkatan strategi deteksi dan pencegahan di era digital.

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis perubahan *modus operandi,* motivasi, serta metode yang digunakan oleh pelaku kejahatan dalam sektor perbankan. Penelitian ini juga mengkaji bagaimana kemajuan teknologi, seperti digitalisasi dan inovasi keuangan, memengaruhi lanskap kejahatan perbankan, sekaligus menilai efektivitas strategi pencegahan dan penegakan hukum yang diterapkan oleh institusi keuangan maupun pemerintah. Mengingat relevansinya terhadap TPPU dan TPPT, studi ini juga menyoroti hubungan erat antara kedua tindak pidana tersebut, di mana teknik-teknik perbankan yang baru memungkinkan peredaran hasil kejahatan menjadi lebih tersembunyi dan cepat, sering kali melibatkan transfer internasional dan transaksi digital.

Meskipun literatur mengenai kejahatan keuangan berbasis siber terus berkembang, masih terdapat sejumlah kesenjangan penelitian yang signifikan. Beberapa studi cenderung memiliki cakupan yang sempit, hanya berfokus pada teknologi tertentu atau wilayah geografis tertentu, sehingga kurang memberikan gambaran komprehensif mengenai tren global dan implikasi lintas batas. Selain itu, terdapat temuan yang saling bertentangan terkait efektivitas kerangka regulasi; sebagian peneliti menekankan sifat progresif dari kebijakan yang ada, sementara yang lain mengkritisi lemahnya penegakan hukum serta kemampuan adaptasi para pelaku kejahatan. Meskipun sebagian besar literatur mengakui meningkatnya ancaman digital, hanya sedikit studi yang memberikan analisis mendalam mengenai respons praktis yang dapat diterapkan oleh institusi perbankan terhadap risiko yang terus berkembang. Studi ini memberikan kontribusi dengan mensintesis temuan-temuan terbaru dan mengidentifikasi area yang masih kurang tereksplorasi, seperti persinggungan antara teknologi finansial (*fintech*), ketertinggalan regulasi (*regulatory lag*), dan skema pencucian uang lintas negara. Studi ini juga memberikan rekomendasi untuk pengembangan penelitian lebih lanjut serta perbaikan kebijakan yang relevan dengan konteks perbankan digital. Melalui pendekatan tinjauan pustaka, penelitian ini bertujuan untuk mengidentifikasi kesenjangan riset yang ada sekaligus memberikan masukan untuk arah penelitian selanjutnya dan praktik kebijakan yang lebih efektif bagi berbagai pemangku kepentingan, termasuk pemerintah, institusi keuangan, dan masyarakat umum. Secara keseluruhan, kontribusi dari studi ini diharapkan dapat mendukung upaya global dalam menciptakan lingkungan perbankan yang lebih aman dari ancaman kejahatan, serta berperan dalam memperkuat pencegahan dan penanggulangan TPPU dan TPPT di era digital.

Pembahasan

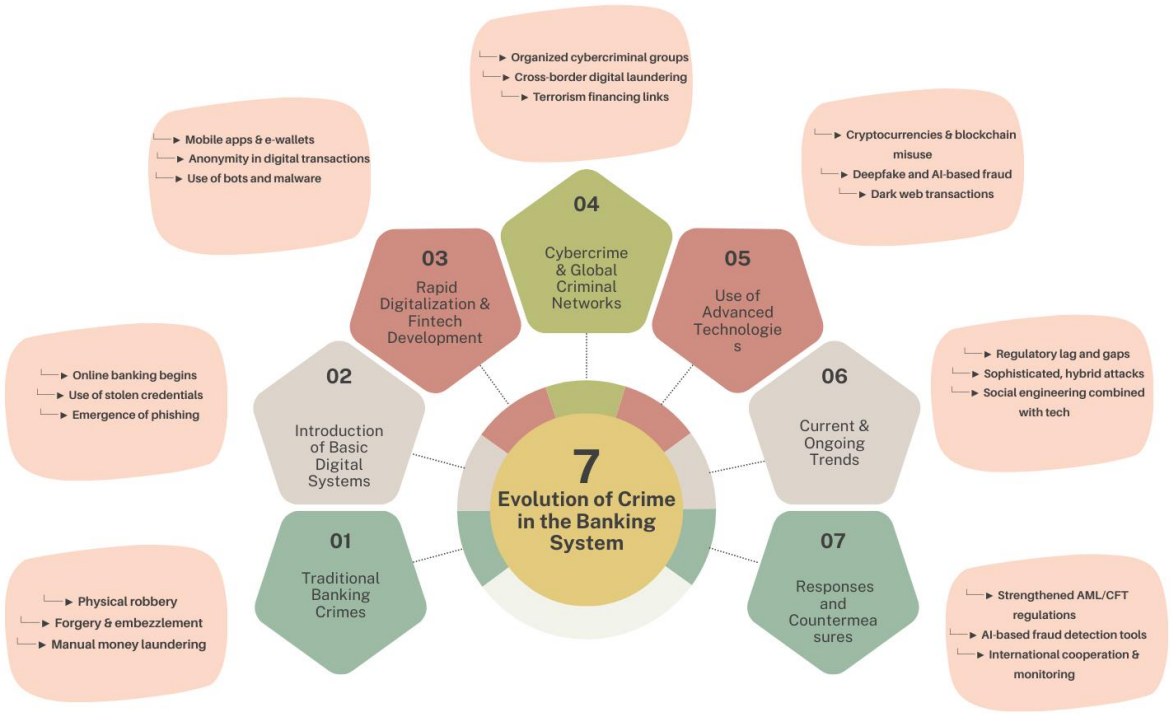
Evolusi Kejahatan dalam Sistem Perbankan

Sejarah kejahatan perbankan telah mengalami evolusi yang signifikan seiring waktu, mencerminkan perubahan dalam teknologi, regulasi, dan dinamika ekonomi global. Pada awal abad ke-20, kejahatan perbankan umumnya terbatas pada praktik seperti penggelapan dana (*embezzlement*) dan manipulasi laporan keuangan, yang sering kali melibatkan pejabat bank atau individu yang memiliki akses ke sistem internal perbankan. Achim dan Borlea menjelaskan bahwa jenis kejahatan ini kerap sulit terdeteksi karena keterbatasan teknologi dan belum adanya mekanisme pengawasan yang efektif.[17] Masciandaro menambahkan bahwa pada masa tersebut, kejahatan perbankan juga erat kaitannya dengan praktik pencucian uang (*money laundering*)

[17] Achim and Borlea, *Economic and Financial Crime*.

dan pemanfaatan pusat keuangan lepas pantai (*offshore financial centers*) untuk menyembunyikan hasil kejahatan.[18]

Pola kejahatan perbankan telah berubah secara drastis seiring dengan kemajuan teknologi dan munculnya sistem perbankan digital. Van Driel mengidentifikasi bahwa era digital telah melahirkan bentuk-bentuk kejahatan baru seperti *hacking*, penipuan identitas, dan skema *phishing*, yang memanfaatkan kerentanan dalam sistem keamanan siber perbankan.[19] Hilal dkk. (2022) mencatat bahwa seiring dengan semakin canggihnya teknologi deteksi anomali, metode penipuan juga terus berkembang agar dapat menghindari deteksi.[20] Wewege, Lee, dan Thomsett menekankan bahwa digitalisasi perbankan membawa peluang dan risiko baru, sehingga menuntut adaptasi cepat terhadap regulasi dan praktik keamanan guna melindungi konsumen dan lembaga keuangan.[21] Sejarah ini menunjukkan bagaimana kejahatan perbankan terus beradaptasi dengan perkembangan teknologi, serta bagaimana regulasi terus berevolusi untuk merespons ancaman yang muncul.



Gambar 1. Evolusi Kejahatan dalam Sistem Perbankan.
Sumber: Disusun oleh penulis, 2024

Kasus klasik penipuan perbankan sering kali melibatkan teknik-teknik kompleks yang mengeksploitasi kelemahan dalam sistem perbankan tradisional. Salah satu contoh terkenal adalah skandal Enron, di mana para eksekutif perusahaan menggunakan praktik akuntansi yang rumit untuk menyembunyikan utang dan secara artifisial meningkatkan laba. Shazeeda Ali mengidentifikasi bahwa pelaku penipuan keuangan semacam ini umumnya memiliki

[18] Donato Masciandaro, *Global Financial Crime: Terrorism, Money Laundering and Offshore Centres* (New York: Taylor & Francis, 2017).

[19] Hugo van Driel, "Financial Fraud, Scandals, and Regulation: A Conceptual Framework and Literature Review," *Business History* 61, no. 8 (2019): 1259–99, https://doi.org/10.1080/00076791.2018.1519026.

[20] Waleed Hilal, S. Andrew Gadsden, and John Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Systems with Applications* 193 (2022): 116429, https://doi.org/10.1016/j.eswa.2021.116429.

[21] Luigi Wewege, Jeo Lee, and Michael C. Thomsett, "Disruptions and Digital Banking Trends," *Journal of Applied Finance & Banking* 10, no. 6 (2020): 15–56.

pemahaman mendalam terhadap kelemahan dalam sistem keuangan serta kemampuan untuk memanipulasi informasi keuangan demi keuntungan pribadi.[22] Dalam kasus Enron, para eksekutif menggunakan serangkaian perusahaan cangkang (*shell companies*) untuk menyembunyikan utang perusahaan, sehingga menampilkan kondisi keuangan yang jauh lebih sehat daripada kenyataan yang ada.

Modus operandi penipuan perbankan klasik juga mencakup skema Ponzi, di mana pelaku menjanjikan keuntungan tinggi kepada investor yang sebenarnya dibayarkan menggunakan dana dari investor baru, bukan dari keuntungan yang sah. Salah satu contoh terkenal adalah kasus Bernie Madoff, yang berhasil menipu ribuan investor selama beberapa dekade. Kwan Choi dkk. (2017) mencatat bahwa skema semacam ini sering kali bergantung pada karisma pelaku serta kemampuannya membangun kepercayaan dengan korban.[23] Pelaku kerap memanfaatkan jaringan sosial dan profesionalnya untuk menarik investor baru, sehingga skema dapat terus berjalan hingga akhirnya runtuh ketika aliran dana baru berhenti.

Di era digital, *modus operandi* penipuan perbankan telah berkembang seiring dengan kemunculan kejahatan siber. Salah satu bentuk yang umum adalah *phishing*, yaitu upaya untuk memperoleh informasi pribadi korban melalui surel atau situs web palsu. Pospisil dkk. (2020) menjelaskan bahwa pelaku sering menggunakan teknik *social engineering* untuk membuat komunikasi tampak sah, misalnya dengan meniru komunikasi dari lembaga keuangan yang dikenal korban.[24] Hal ini membuat korban lebih mudah memberikan informasi sensitif seperti nomor rekening atau kata sandi. *Modus operandi* ini terus berevolusi seiring dengan kemajuan teknologi, di mana pelaku kini juga menggunakan *malware* dan berbagai bentuk serangan siber lainnya untuk mengakses informasi keuangan secara ilegal.

Selain itu, penipuan perbankan dengan *modus operandi* lintas negara (*transnasional*) juga menunjukkan tren peningkatan. Jonathan M. Karpoff menyatakan bahwa dengan adanya globalisasi dan kemajuan teknologi, pelaku kejahatan kini dapat menjalankan skema penipuan dari berbagai lokasi di seluruh dunia, sering kali melibatkan jaringan internasional yang kompleks.[25] Trong Van Nguyen mengungkapkan bahwa dalam banyak kasus, kejahatan ini melibatkan penggunaan identitas palsu dan perusahaan cangkang (*shell companies*) untuk menyamarkan asal-usul dana serta identitas pelaku.[26] Fenomena ini semakin memperumit upaya penegakan hukum dan pengaturan regulasi, karena melibatkan yurisdiksi yang berbeda dan sering kali memanfaatkan celah hukum di berbagai negara.

Transisi menuju era digital telah membawa perubahan besar dalam sistem perbankan. Inovasi teknologi seperti kecerdasan buatan (*artificial intelligence*/AI), *blockchain*, dan *financial technology* (*fintech*) telah menghadirkan efisiensi baru, meningkatkan layanan nasabah, dan mengubah cara transaksi dilakukan. Jakšič dan Marinč menjelaskan bahwa teknologi-teknologi ini telah menyederhanakan proses perbankan dan memungkinkan bank untuk lebih memahami serta melayani nasabah melalui analitik data dan layanan yang dipersonalisasi.[27] Selain itu, teknologi digital seperti *fintech* telah memungkinkan bank untuk menjangkau populasi yang sebelumnya tidak terlayani, sehingga memperluas inklusi keuangan secara global.

Teknologi juga telah mengubah model bisnis perbankan. Perbankan digital telah mengurangi ketergantungan pada kantor cabang fisik dan mempermudah akses layanan melalui perangkat seluler dan platform daring. Mosteanu dan Faccia menyoroti bahwa penggunaan

[22] Ali, "Criminal Minds."

[23] Choi, Lee, and Chun, "Voice Phishing Fraud and Its Modus Operandi."

[24] Pospisil et al., "Modus Operandi in Cybercrime."

[25] Jonathan M. Karpoff, "The Future of Financial Fraud," *Journal of Corporate Finance* 66 (2021): 101694, https://doi.org/10.1016/j.jcorpfin.2020.101694.

[26] Van Nguyen, "The Modus Operandi of Transnational Computer Fraud."

[27] Jakšič and Marinč, "Relationship Banking and Information Technology."

teknologi seperti *blockchain* dalam transaksi keuangan telah meningkatkan transparansi dan keamanan, sementara mata uang kripto (*cryptocurrency*) menawarkan alternatif baru dalam sistem pembayaran dan investasi.[28] Perubahan ini mendorong bank untuk mengadopsi teknologi baru dan mengintegrasikan solusi digital ke dalam operasional mereka guna tetap kompetitif di pasar yang semakin didominasi oleh teknologi.

Kejahatan siber juga mengalami peningkatan yang signifikan seiring dengan kemajuan teknologi dalam sektor perbankan. Kejahatan siber dalam perbankan mencakup berbagai bentuk, seperti *phishing, hacking,* pencurian identitas, dan penyebaran *malware*. Leo dkk.(2019) mencatat bahwa kejahatan-kejahatan ini mengeksploitasi kerentanan dalam sistem keamanan digital bank untuk mengakses informasi sensitif dan dana nasabah.[29] Meskipun teknologi seperti kecerdasan buatan (*artificial intelligence*/AI) dan *machine learning* telah digunakan untuk mendeteksi dan mencegah kejahatan siber, para pelaku juga terus mengembangkan metode baru untuk menghindari deteksi. Hal ini menciptakan semacam "perlombaan senjata" antara pelaku kejahatan dan aparat penegak hukum. Salah satu tantangan utama dalam memberantas kejahatan siber adalah tingkat kompleksitas dan jangkauannya yang bersifat lintas negara. Azernikov dkk. (2018) menunjukkan bahwa kejahatan siber sering kali melibatkan jaringan internasional yang kompleks, sehingga sulit untuk dilacak dan ditindak secara hukum.[30] Selain itu, pelaku kejahatan siber kerap menggunakan teknologi enkripsi dan *dark web* untuk menyamarkan identitas serta aktivitas mereka. Hal ini menyulitkan upaya penegakan hukum dan menuntut kerja sama internasional yang lebih erat dalam pencegahan dan penanggulangan kejahatan siber.

Sejumlah kasus kejahatan siber berskala besar dalam sektor perbankan telah menunjukkan dampak signifikan yang dapat ditimbulkan oleh serangan semacam ini. Salah satu contoh terkenal adalah serangan *ransomware* WannaCry pada tahun 2017, yang memengaruhi banyak organisasi di seluruh dunia, termasuk lembaga keuangan. Wewege, Lee, dan Thomsett mencatat bahwa serangan ini mengunci data korban dan menuntut pembayaran dalam bentuk mata uang kripto, sehingga menyoroti risiko besar yang dihadapi bank di era digital.[31] Serangan tersebut menunjukkan bagaimana kejahatan siber dapat mengganggu operasional bank dan merusak kepercayaan nasabah. Kasus lainnya adalah peretasan sistem SWIFT pada tahun 2016, di mana pelaku berhasil mencuri dana sebesar USD 81 juta dari Bank Sentral Bangladesh. Peristiwa ini menunjukkan bahwa bahkan sistem yang dirancang dengan tingkat keamanan tinggi pun dapat memiliki celah untuk diserang. Kasus tersebut menekankan pentingnya penguatan sistem keamanan serta pengawasan terhadap transaksi keuangan internasional, sekaligus menegaskan perlunya kerja sama antarnegara dalam memberantas kejahatan siber, mengingat keterlibatan pelaku lintas negara dalam serangan tersebut.

Kasus menonjol lainnya adalah *data breach* besar-besaran yang dialami oleh Equifax pada tahun 2017, di mana informasi pribadi lebih dari 147 juta orang berhasil dicuri. Insiden ini menyoroti risiko besar yang terkait dengan penyimpanan dan pengelolaan data digital oleh lembaga keuangan. Navaretti dkk. (2018) menunjukkan bahwa kejadian semacam ini tidak hanya menyebabkan kerugian finansial yang signifikan, tetapi juga berdampak serius terhadap

[28] Narcisa Roxana Mosteanu and Alessio Faccia, "Digital Systems and New Challenges of Financial Management – FinTech, XBRL, Blockchain and Cryptocurrencies," *Quality – Access to Success* 21, no. 174 (2020): 159–66.

[29] Martin Leo, Suneel Sharma, and K. Maddulety, "Machine Learning in Banking Risk Management: A Literature Review," *Risks* 7, no. 1 (2019): 29, https://doi.org/10.3390/risks7010029.

[30] A. D. Azernikov et al., "Innovative Technologies in Combating Cyber Crime," *KnE Social Sciences* 3, no. 2 (2018): 248–52, https://doi.org/10.18502/kss.v3i2.1550.

[31] Wewege, Lee, and Thomsett, "Disruptions and Digital Banking Trends."

reputasi institusi yang terlibat.[32] Hal ini menegaskan pentingnya perlindungan keamanan data dan privasi dalam perbankan digital.

Secara keseluruhan, transisi menuju era digital telah membawa banyak manfaat bagi sistem perbankan, namun juga menciptakan tantangan baru dalam bentuk kejahatan siber. Kejahatan siber terus berkembang seiring dengan kemajuan teknologi, sehingga lembaga perbankan harus senantiasa beradaptasi dan meningkatkan sistem keamanannya guna melindungi aset serta informasi nasabah. Kolaborasi antara perbankan, aparat penegak hukum, dan otoritas pengawas sangat penting untuk merumuskan strategi yang efektif dalam menghadapi ancaman ini dan menjaga integritas sistem keuangan global.

Pola Kejahatan dalam Sistem Perbankan

Karakteristik tindak pidana konvensional (*traditional crimes*) dan tindak pidana siber (*cybercrimes*) dalam konteks perbankan menunjukkan perbedaan yang signifikan dalam hal *modus operandi*, dampak, serta tantangan dalam penegakan hukum. Tindak pidana konvensional, seperti penggelapan dan penipuan, umumnya melibatkan kontak fisik atau interaksi langsung antara pelaku dan korban. Sebagai contoh, kasus penipuan yang melibatkan cek palsu atau penggelapan dana biasanya membutuhkan manipulasi dokumen fisik atau penggunaan identitas palsu secara langsung. Lokanan menjelaskan bahwa kejahatan semacam ini sering dipandang sebagai tindakan yang menyimpang secara moral, di mana pelaku mengejar keuntungan pribadi melalui manipulasi sistem atau penyalahgunaan kepercayaan.[33]

Sebaliknya, tindak pidana siber cenderung terjadi tanpa adanya interaksi fisik antara pelaku dan korban. Kejahatan ini umumnya menggunakan teknologi informasi dan komunikasi sebagai sarana untuk melakukan perbuatan melawan hukum. Contoh yang sering ditemukan termasuk *phishing*, di mana pelaku menipu korban agar memberikan informasi pribadi melalui surel atau situs web palsu, serta serangan *malware* yang merusak atau mencuri data dari sistem komputer. Pospisil dkk. (2020) mencatat bahwa kejahatan siber memiliki karakteristik unik karena dapat dilakukan dari jarak jauh, sehingga memungkinkan pelaku menyembunyikan identitas dan lokasi mereka, yang pada akhirnya mempersulit proses penegakan hukum.[34]

Perbedaan lainnya terletak pada skala dan dampak dari kedua jenis kejahatan tersebut. Tindak pidana konvensional umumnya terbatas pada wilayah geografis tertentu dan sering kali melibatkan jumlah kerugian yang relatif kecil dibandingkan dengan kejahatan siber. Hasham dkk. menunjukkan bahwa kejahatan siber dapat berdampak jauh lebih luas, melibatkan ribuan korban di berbagai negara, dan menyebabkan kerugian finansial yang sangat besar.[35] Contoh serangan *ransomware* seperti WannaCry menunjukkan bagaimana serangan siber dapat melumpuhkan sistem kritis di seluruh dunia dan menyebabkan kerugian hingga miliaran dolar.

Selain itu, kejahatan siber sering kali memanfaatkan teknologi canggih untuk menghindari deteksi dan penuntutan hukum. Choi dkk. (2017) menjelaskan bahwa pelaku kejahatan siber kerap menggunakan teknik seperti enkripsi, *dark web*, dan berbagai alat anonimitas lainnya untuk menyamarkan jejak mereka.[36] Hal ini berbeda dengan tindak pidana konvensional yang umumnya meninggalkan barang bukti fisik atau jejak yang lebih mudah ditelusuri. Payne mencatat bahwa definisi kejahatan siber juga telah berkembang seiring kemajuan teknologi, yang menambah kompleksitas dalam upaya deteksi dan pencegahan kejahatan tersebut.[37]

---

[32] Giorgio Barba Navaretti et al., "Fintech and Banking. Friends or Foes?," *Friends or Foes* (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099337.

[33] Lokanan, "Theorizing Financial Crimes as Moral Actions."

[34] Pospisil et al., "Modus Operandi in Cybercrime."

[35] Hasham, Joshi, and Mikkelsen, *Financial Crime and Fraud in the Age of Cybersecurity*.

[36] Choi, Lee, and Chun, "Voice Phishing Fraud and Its Modus Operandi."

[37] Payne, "Defining Cybercrime."

Tantangan penegakan hukum pun berbeda antara kedua jenis tindak pidana ini. Tindak pidana konvensional umumnya dapat ditangani dengan metode penegakan hukum konvensional, seperti investigasi lapangan dan penangkapan secara fisik. Namun, kejahatan siber memerlukan pendekatan yang lebih teknis dan sering kali melibatkan kerja sama internasional karena sifatnya yang lintas batas negara. Fahlevi dkk. menyoroti bahwa negara-negara seperti Indonesia menghadapi tantangan tersendiri dalam menangani kejahatan siber, terutama karena keterbatasan infrastruktur teknologi dan kurangnya sumber daya manusia yang memiliki keahlian di bidang kejahatan digital.[38]

Terakhir, kejahatan siber memiliki potensi untuk terus berkembang seiring dengan kemunculan teknologi baru seperti mata uang kripto dan teknologi blockchain. Trozze dkk. (2022) mencatat bahwa mata uang kripto dapat digunakan untuk membiayai atau menyembunyikan hasil kejahatan siber, sehingga membuat aliran dana menjadi lebih sulit dilacak.[39] Kejahatan semacam ini memerlukan pendekatan regulatif dan penegakan hukum yang inovatif untuk mencegah dan menangani ancaman yang terus berkembang. Secara keseluruhan, perbedaan karakteristik antara kejahatan konvensional dan kejahatan siber menunjukkan perlunya adaptasi dalam strategi penegakan hukum dan kebijakan keamanan guna menjawab tantangan di era digital saat ini.

Kejahatan siber dalam sektor perbankan mencakup berbagai bentuk serangan yang bertujuan untuk mencuri data, dana, atau merusak sistem perbankan. Tindak pidana ini dapat berdampak signifikan terhadap individu, pelaku usaha, maupun lembaga keuangan. Salah satu teknik yang umum digunakan oleh pelaku adalah *phishing* dan rekayasa sosial (*social engineering*), yakni metode untuk menipu korban agar secara sukarela memberikan informasi pribadi atau keuangan mereka. Phishing biasanya dilakukan melalui email atau pesan singkat yang tampak seolah-olah berasal dari institusi terpercaya, seperti bank atau perusahaan teknologi, dengan tujuan memperoleh akses ke akun pengguna. Gomes dkk. (2020) menjelaskan bahwa serangan *phishing* memanfaatkan tingkat kepercayaan korban terhadap lembaga yang dihormati, sehingga korban terdorong untuk mengeklik tautan atau membuka lampiran yang bersifat berbahaya.[40] Sementara itu, *social engineering* merupakan bentuk manipulasi psikologis yang dilakukan untuk mengelabui individu agar mengungkapkan informasi sensitif atau melakukan tindakan tertentu yang berpotensi membahayakan sistem keamanan.

Rekayasa sosial (*social engineering)* tidak selalu melibatkan penggunaan teknologi canggih, melainkan lebih menitikberatkan pada eksploitasi kelemahan manusia, seperti rasa percaya diri yang berlebihan atau kurangnya pengetahuan mengenai ancaman keamanan digital. Spoorthi dkk menunjukkan bahwa taktik ini sangat efektif dalam konteks *e-banking*, di mana pengguna sering kali tidak menyadari risiko siber yang mengancam.[41] Sebagai contoh, pelaku dapat menghubungi korban melalui sambungan telepon dan menyamar sebagai petugas bank untuk memperoleh data kredensial, seperti nama pengguna dan kata sandi. Serangan seperti ini dapat menyebabkan kerugian finansial yang besar serta merusak reputasi institusi keuangan yang menjadi sasaran.

Pencurian identitas dan data merupakan salah satu bentuk tindak pidana siber, di mana pelaku memperoleh akses secara tidak sah terhadap informasi pribadi atau keuangan seseorang dengan maksud untuk menyalahgunakannya. Informasi yang dicuri dapat berupa nomor kartu

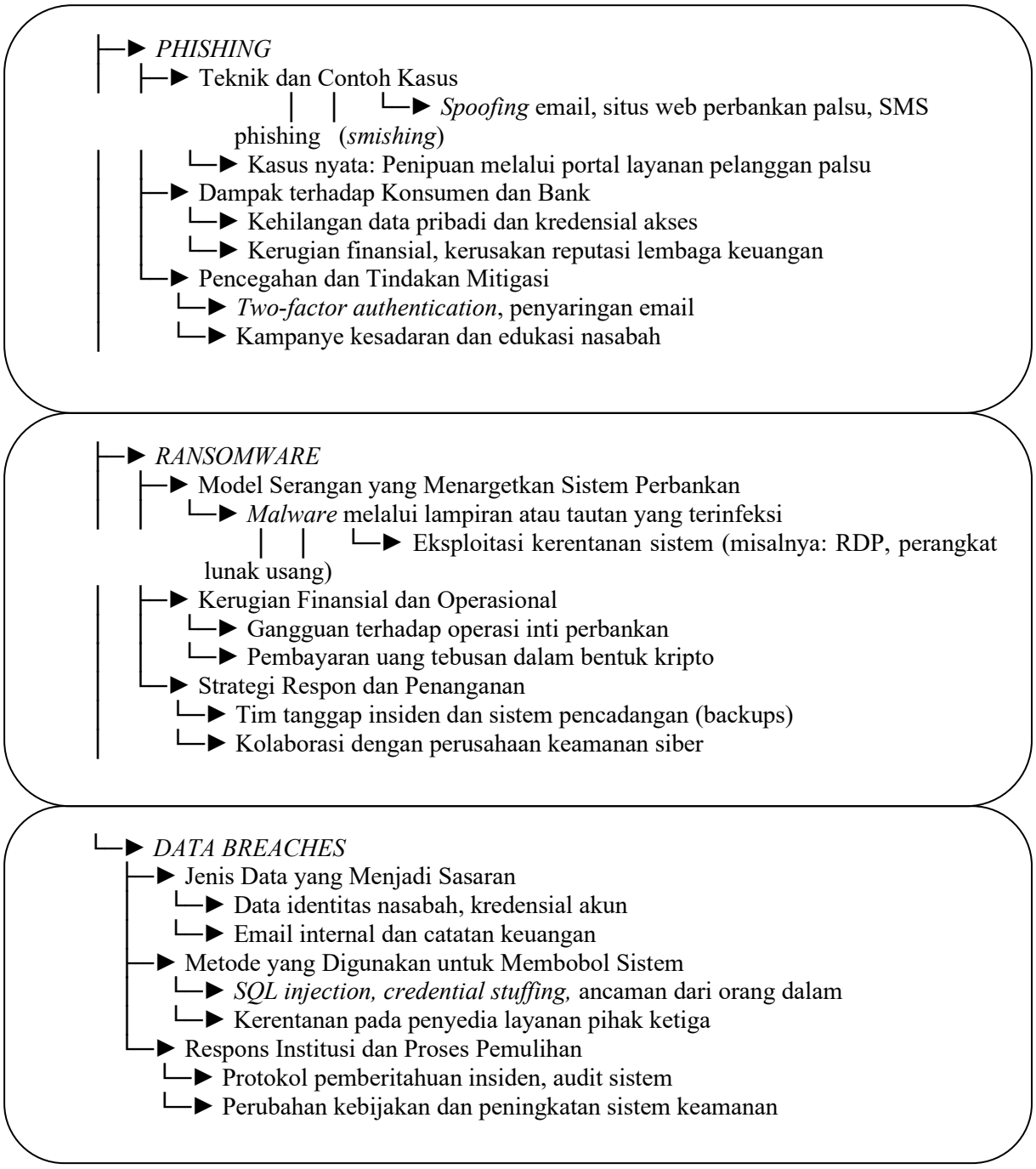
[38] Fahlevi et al., "Cybercrime Business Digital in Indonesia."

[39] Trozze et al., "Cryptocurrencies and Future Financial Crime."

[40] Vanessa Gomes, Joaquim Reis, and Bráulio Alturas, "Social Engineering and the Dangers of Phishing," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)* (IEEE, 2020), 1–7, https://ieeexplore.ieee.org/abstract/document/9140445/.

[41] M. Spoorthi et al., "Impacts of Social Engineering on E-Banking," in *Social Engineering in Cybersecurity*, ed. H. L. Gururaj, V. Janhavi, and V. Ambika (Boca Raton: CRC Press, 2024), 85–118.

kredit, data rekening bank, atau data pribadi lainnya. Burnes dkk. menyatakan bahwa pencurian identitas umumnya terjadi melalui serangan *phishing* atau kebocoran data berskala besar *(data breach*), di mana pelaku berhasil membobol basis data yang menyimpan informasi sensitif milik pengguna.[42] Data yang diperoleh secara ilegal tersebut kemudian dapat diperjualbelikan di pasar gelap (*black market*) atau digunakan untuk melakukan penipuan (*fraud*) dan tindak kejahatan keuangan lainnya.



Gambar 2. Kejahatan Siber dalam Perbankan Digital.

[42] David Burnes, Marguerite DeLiema, and Lynn Langton, "Risk and Protective Factors of Identity Theft Victimization in the United States," *Preventive Medicine Reports* 17 (2020): 101058, https://doi.org/10.1016/j.pmedr.2020.101058.

Sumber: Modifikasi dari Karpoff (2021)[43] dan Haitham M. Alzoubi dkk. (2022)[44]

Keamanan data merupakan aspek krusial dalam pencegahan tindak pidana pencurian identitas. Nicholls dkk. (2021) menekankan bahwa lembaga perbankan wajib menerapkan langkah-langkah pengamanan yang kuat, seperti enkripsi data dan otentikasi dua faktor (*two-factor authentication*), guna melindungi informasi nasabah.[45] Namun demikian, meskipun telah diterapkan pengamanan yang ketat, kebocoran data (*data leak*) tetap dapat terjadi, baik akibat kelemahan teknis maupun kesalahan manusia (*human error*). Hal ini menunjukkan perlunya tingkat kewaspadaan dan kesadaran yang tinggi dari seluruh pihak yang terlibat, baik institusi maupun pengguna layanan.

Peretasan (*hacking*) dan pelanggaran data (*data breaches*) merupakan bentuk serangan siber di mana pelaku memperoleh akses tanpa izin ke dalam sistem atau jaringan komputer untuk mencuri, memodifikasi, atau menghancurkan data. Alzoubi dkk. (2022) menjelaskan bahwa serangan semacam ini dapat dilakukan melalui berbagai metode, termasuk penggunaan perangkat peretasan (*hacking tools*), eksploitasi kerentanan perangkat lunak, atau manipulasi protokol jaringan.[46] Pelanggaran data umumnya menyebabkan eksfiltrasi informasi sensitif secara besar-besaran, yang kemudian dapat dimanfaatkan untuk berbagai tujuan ilegal, termasuk pencurian identitas dan penipuan (*fraud*).

Kasus peretasan berskala besar, seperti data breach yang menimpa Equifax, menunjukkan seberapa merusak dampak dari serangan siber semacam ini. Pratama dkk. mencatat bahwa insiden tersebut menyebabkan terekspos nya data pribadi jutaan orang, yang kemudian dimanfaatkan untuk aktivitas kriminal.[47] Pelanggaran data tidak hanya menimbulkan kerugian finansial langsung, tetapi juga merusak reputasi perusahaan serta melemahkan kepercayaan publik terhadap keamanan sistem digital.

Ransomware dan *malware* merupakan jenis perangkat lunak berbahaya (*malicious software*) yang dirancang untuk merusak atau mengambil alih sistem komputer. *Ransomware* bekerja dengan cara mengenkripsi data pada komputer korban dan kemudian menuntut pembayaran tebusan untuk memulihkan akses tersebut. Karpoff mencatat bahwa serangan *ransomware* semakin berkembang secara teknis, dengan pelaku sering kali menyasar lembaga keuangan dan infrastruktur kritis lainnya.[48] Setelah sistem terinfeksi, korban biasanya dipaksa membayar tebusan dalam bentuk mata uang kripto yang sulit dilacak demi mendapatkan kunci dekripsi.

Sementara itu, *malware* mencakup berbagai jenis perangkat lunak jahat yang dirancang untuk mencuri data, memantau aktivitas pengguna, atau merusak sistem. Ghelani dkk. (2022) menjelaskan bahwa *malware* dapat diinstal melalui email *phishing*, unduhan berbahaya, atau situs web yang telah terinfeksi.[49] *Malware* dapat menyebabkan kerugian yang signifikan, termasuk pencurian data, kegagalan sistem, dan kerugian finansial. Dalam beberapa kasus,

[43] Karpoff, "The Future of Financial Fraud."

[44] Haitham M. Alzoubi et al., "Cyber Security Threats on Digital Banking," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (IEEE, 2022), 1–4, https://ieeexplore.ieee.org/abstract/document/9896966/.

[45] Jack Nicholls, Aditya Kuppa, and Nhien-An Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape," *Ieee Access* 9 (2021): 163965–86.

[46] Haitham M. Alzoubi et al., "Cyber Security Threats on Digital Banking," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (IEEE, 2022), 1–4, https://ieeexplore.ieee.org/abstract/document/9896966/.

[47] Pratama et al., "Cybercrime."

[48] Karpoff, "The Future of Financial Fraud."

[49] Diptiben Ghelani, Tan Kian Hua, and Surendra Kumar Reddy Koduru, "Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking," *American Journal of Computer Science and Technology* (2022): 1–8, https://doi.org/10.22541/au.166385206.63311335/v1.

malware juga digunakan sebagai bagian dari serangan yang lebih besar, seperti peretasan sistem (*system hack*) atau pelanggaran data (*data breach*).

Kajian mengenai kejahatan dalam sektor perbankan tidak boleh hanya berfokus pada tindak pidana konvensional yang telah beradaptasi dengan teknologi digital (*cyber-enabled crimes*), seperti penipuan dan tindak pidana pencucian uang (*money laundering*) yang dilakukan melalui platform daring, tetapi juga harus mencermati kemunculan bentuk kejahatan baru yang sepenuhnya bergantung pada eksistensi teknologi digital (*cyber-dependent crimes*). *Cyber-enabled crimes* biasanya memanfaatkan alat digital untuk memperluas cakupan kejahatan konvensional. Sebagai contoh, skema *phishing* yang dilakukan melalui email atau situs palsu bertujuan mencuri kredensial pengguna. Tindak pidana ini menggunakan internet sebagai media, tetapi tidak sepenuhnya bergantung padanya untuk dapat terjadi. Perkembangan jenis kejahatan ini menunjukkan bahwa motif kriminal klasik dapat mengambil dimensi baru ketika dipadukan dengan kemajuan teknologi.

Sebaliknya, *cyber-dependent crimes* merupakan tantangan yang lebih baru dan kompleks karena hanya dapat terjadi dengan adanya infrastruktur digital. Contohnya termasuk serangan *Distributed Denial-of-Service* (DDoS), *ransomware*, *data breach*, dan *cryptojacking*, yang menargetkan kerentanan sistem, data keuangan, atau jaringan institusi. Tindak pidana ini memerlukan lingkungan digital untuk beroperasi dan sering kali melibatkan pengetahuan teknis yang tinggi serta koordinasi lintas negara. Kemunculan kejahatan jenis ini menyoroti kebutuhan mendesak bagi para pembuat kebijakan dan institusi perbankan untuk menyadari bahwa strategi keamanan tidak cukup hanya dengan memperbarui metode konvensional, tetapi juga harus mengantisipasi serta merespons risiko dari kejahatan yang sepenuhnya lahir dari era digital. Pendekatan ganda ini sangat penting untuk melindungi sistem keuangan serta menjaga kepercayaan publik dalam dunia yang semakin terdigitalisasi.

Secara keseluruhan, kejahatan siber dalam sektor perbankan terus berkembang seiring dengan kemajuan teknologi dan meningkatnya kompleksitas sistem digital. Bank dan lembaga keuangan harus tetap waspada dan secara berkala memperbarui langkah-langkah keamanan guna melindungi data dan aset dari berbagai ancaman siber. Kesadaran dan edukasi pengguna juga menjadi kunci dalam pencegahan, mengingat banyak serangan siber yang mengeksploitasi kelemahan manusia.

Tabel 1 menggambarkan beragam metode kejahatan yang dilakukan oleh pelaku serta jenis korban yang umumnya menjadi sasaran. Pola-pola ini mencerminkan spektrum ancaman yang luas yang dihadapi oleh individu maupun organisasi di era digital. Hasil dari tabel pola kejahatan berdasarkan pelaku dan korban menunjukkan bahwa kejahatan dalam sistem perbankan dapat diklasifikasikan ke dalam beberapa kategori utama berdasarkan entitas yang terlibat. Dari sisi pelaku, individu merupakan pelaku paling umum, terutama dalam kasus penipuan sederhana seperti *phishing* dan pencurian identitas. Kelompok kejahatan terorganisir menonjol dalam kejahatan yang lebih kompleks seperti tindak pidana pencucian uang dan peretasan sistem berskala besar. Aktor negara (*state actors*), meskipun relatif jarang, memiliki dampak yang signifikan, khususnya dalam kasus spionase ekonomi dan serangan siber yang disponsori oleh negara (*state-sponsored cyberattacks*). Dari sisi korban, individu sering menjadi target dalam kejahatan penipuan dan pencurian data, sedangkan perusahaan, termasuk bank dan lembaga keuangan lainnya, lebih rentan terhadap serangan siber berskala besar seperti *ransomware* dan peretasan sistem.

Tabel 1 menunjukkan bahwa evolusi teknologi telah mengubah lanskap kejahatan perbankan, di mana semakin banyak pelaku yang menggunakan teknologi canggih untuk melancarkan aksinya. Hal ini tercermin dari meningkatnya jumlah kasus yang melibatkan kelompok kejahatan terorganisir dan aktor negara yang menggunakan metode yang lebih kompleks dan sulit dilacak. Pelaku perorangan juga menunjukkan kemampuan adaptasi dengan beralih dari penipuan langsung ke serangan berbasis siber yang lebih terfokus. Dari sisi korban,

individu tetap menjadi pihak yang rentan terhadap berbagai bentuk penipuan, namun perusahaan mengalami peningkatan kerugian finansial maupun reputasi akibat serangan siber. Data ini mengindikasikan perlunya strategi keamanan yang lebih komprehensif dan adaptif, baik di tingkat individu maupun institusi, untuk menghadapi ancaman yang terus berkembang di era digital.

Tabel 1. Pola Kejahatan Berdasarkan Pelaku dan Korban.

Pola Kejahatan	Pelaku	Korban	Deskripsi
Phishing	Peretas (*hacker*) atau penipu (*scammer*)	Individu, nasabah bank	Serangan yang berusaha memperoleh informasi pribadi dengan menyamar sebagai entitas tepercaya melalui email atau pesan palsu.
Social Engineering	Manipulator	Pegawai bank, nasabah	Teknik manipulasi psikologis untuk memperoleh informasi sensitif dengan mengeksploitasi kepercayaan atau ketidaktahuan korban terhadap ancaman keamanan.
Pencuri Identitas	Pelaku kejahatan siber (*Cybercriminals*)	Individu, nasabah bank	Pencurian informasi pribadi untuk mengakses akun atau mencuri identitas guna digunakan dalam aktivitas ilegal.
Data Breach	*Hacker*	Lembaga keuangan	Akses tidak sah terhadap data perusahaan atau nasabah melalui pelanggaran terhadap sistem keamanan informasi.
Ransomware	*Cybercriminals*	Lembaga keuangan, individu	Serangan yang mengenkripsi data milik korban dan meminta tebusan untuk memberikan kunci dekripsi guna memulihkan akses data tersebut.
Malware	*Hackers* atau pembuat *malware*	Individu, perusahaan	Perangkat lunak berbahaya yang digunakan untuk mencuri data, memata-matai pengguna, atau merusak sistem komputer.
System Hacking	*Hacker*	Lembaga keuangan, perusahaan	Tindakan memperoleh akses ilegal ke dalam sistem komputer atau jaringan untuk mencuri data atau melakukan sabotase sistem.
Penipuan (*Fraud*)	*Fraudster*	Individu, perusahaan	Penggunaan informasi palsu atau dimanipulasi untuk mendapatkan keuntungan finansial atau materiil secara melawan hukum.
Penipuan Kartu Kredit	*Fraudster*	Individu, nasabah bank	Pencurian informasi kartu kredit untuk digunakan dalam pembelian ilegal atau penggelapan dana

Penipuan Investasi	*Scammer*, pengelola dana ilegal	Individu, investor	Penawaran peluang investasi palsu atau penipuan terhadap investor agar menyetorkan dana dengan janji imbal hasil yang tidak nyata.

Sumber: Data olahan, 2024

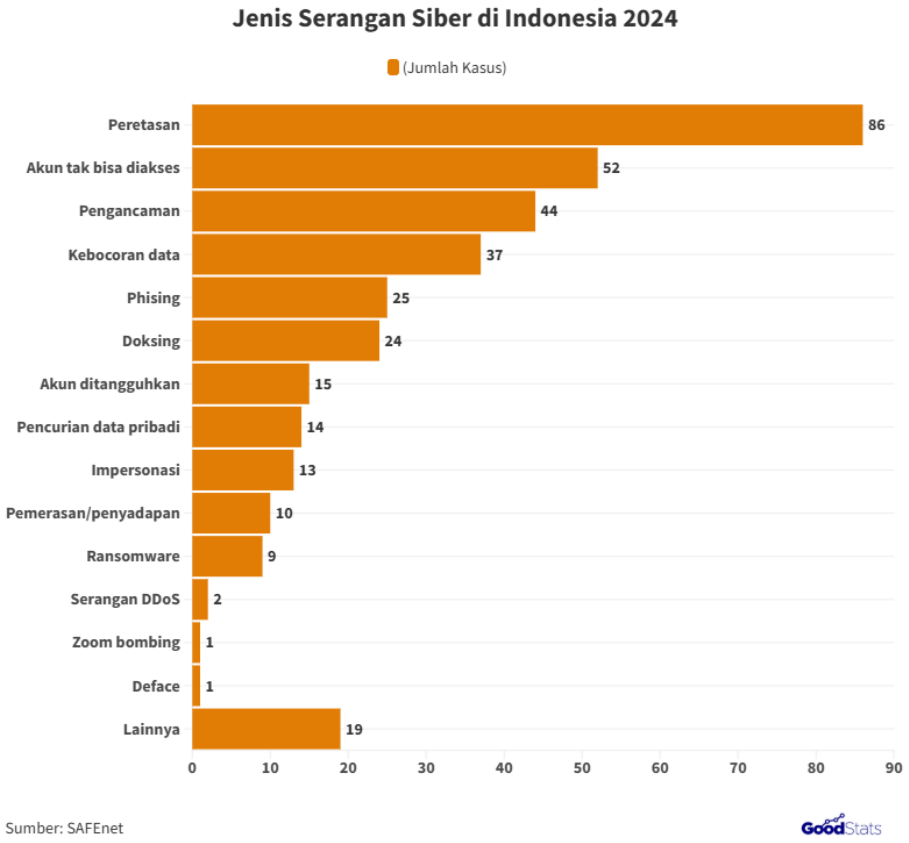
Tabel 2. Motif dan Tujuan Tindak Kejahatan.

Tipe Kejahatan	Motif	Tujuan
Phishing	Keuntungan finansial	Memperoleh informasi pribadi untuk mencuri uang atau menyalahgunakan identitas
Social Engineering	Manipulasi psikologis, keuntungan pribadi	Mengecoh korban agar memberikan informasi sensitif atau akses ke sistem
Pencuri Identitas	Keuntungan finansial, penyamaran identitas	Mengakses akun dan memperoleh keuntungan dengan menggunakan identitas palsu
Data Breach	Keuntungan finansial, sabotase	Mengambil data sensitif untuk dijual atau digunakan secara ilegal, serta mengganggu operasional
Ransomware	Pemerasan	Memaksa korban membayar tebusan untuk mendapatkan kembali akses terhadap data
Malware	Spionase, keuntungan finansial	Menginfeksi sistem untuk mencuri data, memata-matai, atau merusak sistem
System Hacking	Keuntungan finansial, tantangan teknis atau ideologis	Mengakses sistem untuk mencuri data, merusak, atau unjuk keterampilan teknis
Penipuan (*Fraud*)	Keuntungan finansial, manipulasi informasi	Menipu korban untuk mendapatkan uang atau barang secara tidak sah
Penipuan Kartu Kredit	Keuntungan finansial	Menggunakan informasi kartu kredit untuk melakukan transaksi ilegal
Penipuan Investasi	Keuntungan finansial	Menipu investor agar menanamkan uang dalam skema investasi palsu

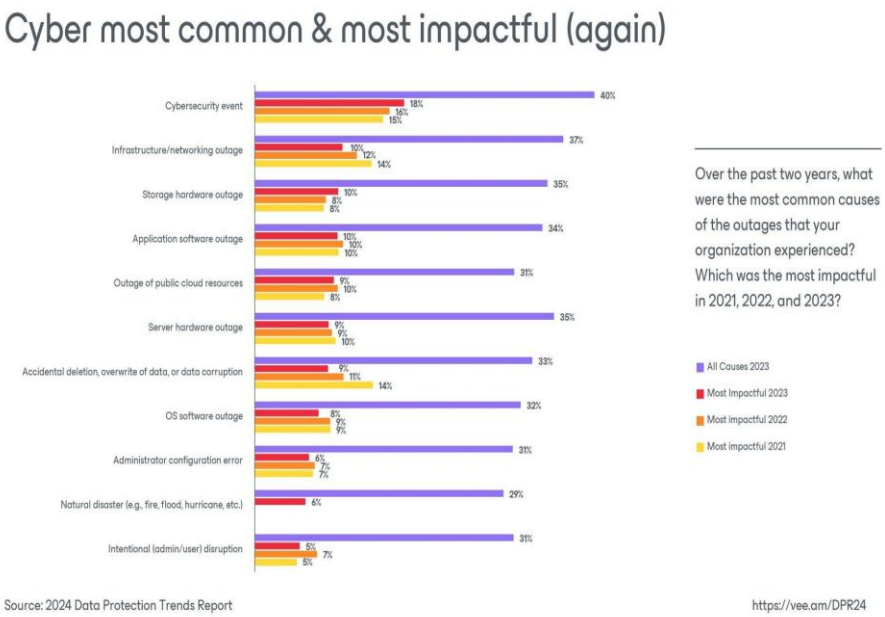
Sumber: Data olahan, 2024

Tabel 2 mengidentifikasi berbagai alasan di balik tindakan kriminal dalam sistem perbankan. Berdasarkan data yang disajikan, motif ekonomi merupakan yang paling dominan, di mana pelaku umumnya menginginkan keuntungan finansial secara cepat dan mudah. Motif ini mencakup tindak pidana seperti pencurian dana, tindak pidana pencucian uang (TPPU), dan penggelapan. Selain itu, ditemukan pula motif politik, khususnya dalam kasus yang melibatkan aktor negara atau kelompok kejahatan terorganisir, di mana tujuannya dapat mencakup upaya untuk mendestabilisasi perekonomian atau merusak reputasi suatu negara tertentu. Tujuan lain yang teridentifikasi termasuk sabotase sistem, yang sering kali dimaksudkan untuk merusak infrastruktur keuangan atau menimbulkan kerugian terhadap target tertentu.

Analisis terhadap data mengenai motif dan tujuan menunjukkan bahwa kejahatan finansial tidak semata-mata didorong oleh keinginan untuk memperoleh keuntungan ekonomi, tetapi juga dapat memiliki dimensi politik dan strategis. Dominasi motif ekonomi mencerminkan kerentanan sistem keuangan terhadap eksploitasi oleh individu atau kelompok yang mencari keuntungan secara ilegal. Namun, keberadaan motif politik dan sabotase menunjukkan bahwa sistem perbankan juga dapat menjadi target dalam konteks konflik yang lebih luas, termasuk konflik antarnegara atau serangan oleh kelompok ekstremis. Hal ini menegaskan pentingnya pendekatan keamanan yang komprehensif, yang tidak hanya berfokus pada pencegahan pencurian dan penipuan, tetapi juga pada perlindungan terhadap ancaman yang lebih luas dan kompleks. Temuan ini menunjukkan perlunya kebijakan keamanan yang lebih holistik, termasuk peningkatan kerja sama internasional serta penguatan regulasi dan teknologi dalam menghadapi berbagai jenis ancaman yang dihadapi oleh sistem perbankan.



Gambar 3. Jenis-jenis Serangan Siber di Indonesia Tahun 2024.
Sumber: SAFEnet



Gambar 4. Serangan Siber Paling Umum dan Paling Berdampak.
Sumber: Laporan Tren Perlindungan Data 2024

Tabel 3. Dampak Tindak Kejahatan di Sektor Perbankan.

Jenis Kejahatan	Dampak pada Korban	Dampak pada Lembaga Keuangan	Dampak pada Ekonomi dan Masyarakat
Phishing	Kehilangan uang, pencurian identitas, kerugian emosional	Kerusakan reputasi, biaya pemulihan, penurunan kepercayaan nasabah	Penurunan kepercayaan publik, peningkatan biaya keamanan
Social Engineering	Kehilangan informasi sensitif, kerugian finansial	Kehilangan data, pelanggaran privasi	Ketidakpercayaan terhadap teknologi dan layanan daring
Pencuri Identitas	Penyalahgunaan identitas, kerugian finansial	Peningkatan klaim penipuan, biaya penanganan	Peningkatan insiden penipuan, beban pada sistem hukum
Data Breach	Kehilangan privasi, potensi kerugian finansial	Kerusakan reputasi, gugatan hukum, biaya pemulihan	Kehilangan data pelanggan, berdampak pada keamanan data
Ransomware	Kehilangan akses data, potensi kerugian finansial	Gangguan operasional, pembayaran tebusan, kerugian finansial	Peningkatan biaya keamanan, dampak terhadap perekonomian lokal
Malware	Kehilangan data pribadi, kerusakan perangkat	Kegagalan sistem, biaya pemulihan	Peningkatan biaya keamanan, dampak terhadap perekonomian lokal
System Hacking	Kehilangan data, kerugian finansial	Gangguan layanan, kehilangan data kritikal	Ketidakstabilan sistem keuangan, peningkatan biaya keamanan

Penipuan (*Fraud*)	Kehilangan uang, kerugian emosional	Peningkatan klaim penipuan, kerugian finansial	Penurunan kepercayaan konsumen, berdampak pada pasar
Penipuan Kartu Kredit	Kehilangan uang, beban pembuktian untuk membela diri	Biaya penggantian, peningkatan pengawasan transaksi	Peningkatan biaya transaksi, berdampak pada kepercayaan konsumen
Penipuan Investasi	Kehilangan investasi, kerugian finansial besar	Reputasi buruk, berkurangnya minat investor	Peningkatan ketidakpercayaan terhadap pasar investasi, berdampak pada perekonomian

Sumber: Data olahan, 2024

Tabel 3 menggambarkan berbagai konsekuensi yang timbul akibat aktivitas kriminal di sektor keuangan. Dampak-dampak ini mencakup kerugian finansial langsung, seperti hilangnya dana nasabah atau dana bank, serta biaya yang dikeluarkan untuk menangani akibat dari insiden tersebut. Selain itu, tabel ini juga mencantumkan kerugian non-finansial, seperti rusaknya reputasi lembaga keuangan, yang dapat menyebabkan hilangnya kepercayaan nasabah dan penurunan nilai pasar. Dampak psikologis juga dapat terjadi, di mana korban mengalami stres atau trauma akibat kehilangan uang atau pencurian identitas. Dampak-dampak ini tidak hanya dirasakan oleh individu atau entitas yang menjadi korban langsung, tetapi juga dapat memengaruhi perekonomian secara keseluruhan, misalnya melalui penurunan stabilitas keuangan.

Analisis terhadap dampak kejahatan perbankan menunjukkan bahwa konsekuensinya bersifat kompleks dan meluas. Selain kerugian finansial secara langsung, dampak jangka panjang seperti rusaknya reputasi dan hilangnya kepercayaan publik memiliki implikasi serius terhadap stabilitas keuangan dan kepercayaan terhadap sistem perbankan secara keseluruhan. Sebagai contoh, lembaga keuangan yang mengalami serangan atau terlibat dalam skandal dapat kehilangan nasabah, yang pada akhirnya mengurangi pendapatan dan profitabilitas serta menciptakan ketidakstabilan di industri perbankan secara umum. Efek domino ini tidak hanya memengaruhi institusi yang terlibat secara langsung, tetapi juga dapat mengikis kepercayaan publik terhadap sistem keuangan secara menyeluruh.

Kejahatan perbankan juga sering kali berkaitan erat dengan Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT), karena pelaku kejahatan memanfaatkan kelemahan dalam sistem untuk menyamarkan asal-usul dana ilegal atau mendukung aktivitas terlarang. Misalnya, metode pencucian uang yang kompleks sering kali memanfaatkan transaksi lintas negara dan platform digital, yang kerap menyulitkan otoritas dalam menelusuri aliran dana dan membuka peluang penyalahgunaan sistem perbankan. Dampak jangka panjang dari skema tersebut mencakup meningkatnya risiko keamanan nasional dan global, sehingga diperlukan sistem pengawasan yang lebih kuat serta upaya lintas batas negara untuk mengidentifikasi dan mencegah aktivitas semacam itu. Hal ini memperkuat urgensi bagi perbankan dan regulator untuk bekerja sama dalam memperkuat sistem keamanan dan membangun kebijakan pencegahan yang adaptif guna menjaga integritas dan kepercayaan publik terhadap sektor perbankan di era digital.

Kejahatan perbankan sering kali memiliki keterkaitan erat dengan Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT), karena pelaku kejahatan memanfaatkan kerentanan sistemik untuk menyamarkan asal-usul dana ilegal atau memfasilitasi aktivitas terlarang. Teknik pencucian uang yang canggih—seperti *layering* melalui transfer lintas negara, penggunaan perusahaan cangkang (*shell companies*), dan integrasi melalui sistem pembayaran digital—menciptakan jejaring keuangan yang kompleks

dan menyulitkan upaya pemantauan baik di tingkat nasional maupun internasional. Di Indonesia, Afriansyah dkk. menyoroti evolusi kerangka hukum dan kelembagaan dalam menangani pendanaan terorisme, serta menekankan pentingnya penguatan kerja sama intelijen keuangan dan penegakan regulasi. Digitalisasi sistem perbankan, meskipun membawa kemudahan, juga memperluas cakupan risiko, dengan memungkinkan arus dana yang lebih cepat, anonim, dan lintas batas yang dapat dieksploitasi untuk kepentingan TPPT.[50]

Dinamika ini menunjukkan urgensi akan perlunya kerangka pencegahan yang kokoh dan kolaborasi lintas lembaga. Seperti disampaikan oleh Broby, pertumbuhan pesat teknologi keuangan (*fintech*) menuntut adanya peninjauan ulang terhadap model risiko dan kapasitas regulasi, karena mekanisme pengawasan konvensional semakin tidak memadai.[51] Sebagai tanggapan, Meiryani dkk. (2023) menekankan pentingnya peran *Regulatory Technology* (*RegTech*) yang semakin relevan, karena memungkinkan pemantauan secara *real-time* dan kepatuhan otomatis untuk menghadapi ancaman TPPU dan TPPT di sektor perbankan Indonesia.[52] Dengan demikian, menjaga kepercayaan publik dan melindungi integritas sistem perbankan di era digital membutuhkan pendekatan yang proaktif dan adaptif, yang menyelaraskan kerangka hukum, pemanfaatan teknologi, dan kerja sama internasional dalam upaya pemberantasan kejahatan keuangan.

Transformasi Pola Kejahatan Perbankan dan Kaitannya dengan TPPU dan TPPT

Perkembangan teknologi dalam sistem perbankan telah secara signifikan mengubah pola kejahatan perbankan, menjadikannya semakin kompleks dan sulit untuk dideteksi. Seiring dengan digitalisasi layanan perbankan, berbagai bentuk kejahatan berbasis teknologi—seperti peretasan (*hacking*), *phishing*, dan penipuan digital—mengalami peningkatan. Fenomena ini tidak hanya berdampak pada ancaman terhadap keamanan perbankan, tetapi juga meningkatkan risiko terjadinya Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT). Dalam konteks internasional, laporan dari Financial Action Task Force (FATF) menyatakan bahwa kejahatan siber dan kejahatan perbankan sering kali dimanfaatkan sebagai sarana untuk melakukan TPPU dan TPPT, mengingat karakteristiknya yang lintas batas serta penggunaan anonimitas digital. Di Indonesia, kasus yang menimpa PT Bank Rakyat Indonesia (Persero) Tbk pada tahun 2018, yang melibatkan pencurian data nasabah, menjadi contoh nyata bahwa lembaga perbankan nasional masih rentan terhadap kejahatan digital yang berpotensi terkait dengan TPPU dan TPPT.[53]

Keunggulan teknologi dalam sistem perbankan juga menciptakan celah yang dieksploitasi oleh pelaku TPPU dan TPPT. Dalam kasus internasional, skandal Panama Papers pada tahun 2016 mengungkap jaringan perusahaan cangkang (*shell companies*) yang digunakan untuk menghindari pajak dan mencuci uang oleh sejumlah elit dunia. Skema perusahaan cangkang tersebut melibatkan perbankan sebagai saluran untuk menyamarkan aliran dana ilegal, menunjukkan bagaimana sistem perbankan dapat dimanfaatkan untuk tujuan pencucian uang

[50] Arie Afriansyah, Ahmad Ghozi, and M Akila Wargadalem, "Indonesia's Laws and Policies in Combatting Terrorism Financing: An Update Analysis," *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2, no. 1 (2023): 1–18, https://doi.org/10.59593/amlcft.2023.v2i1.49.

[51] Daniel Broby, "Financial Technology and the Future of Banking," *Financial Innovation* 7, no. 1 (2021): 47, https://doi.org/10.1186/s40854-021-00264-y.

[52] Meiryani Meiryani, Gatot Soepriyanto, and Jessica Audrelia, "Effectiveness of Regulatory Technology Implementation in Indonesian Banking Sector to Prevent Money Laundering and Terrorist Financing," *Journal of Money Laundering Control* 26, no. 4 (2022): 892–908, https://doi.org/10.1108/JMLC-04-2022-0059.

[53] Mohammad Fadil Imran, "Preventing and Combating Cybercrime in Indonesia," *International Journal of Cyber Criminology* 17, no. 1 (2023): 223–35.

dalam skala global.[54] Di Indonesia sendiri, sejumlah kasus TPPU yang berkaitan dengan korupsi juga telah terungkap. Salah satunya adalah kasus korupsi proyek e-KTP, di mana hasil kejahatan dialirkan melalui beberapa bank nasional sebelum akhirnya disamarkan atau diinvestasikan.[55]

Penggunaan teknologi canggih dalam modus Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT) terus berkembang. Salah satu metode yang semakin populer adalah penggunaan mata uang digital (*cryptocurrency*), yang sulit dilacak oleh otoritas. Dalam sebuah studi kasus di Amerika Serikat, investigasi oleh FBI pada tahun 2021 mengungkap bahwa kelompok kejahatan internasional memanfaatkan *cryptocurrency* untuk menyembunyikan dana hasil tindak pidana, termasuk pendanaan terorisme.[56] Hal ini dimungkinkan karena sifat pseudonim dan sulit dilacak dari transaksi kripto, yang memungkinkan transfer dana secara cepat dan anonim. Di Indonesia, Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) telah memberikan peringatan mengenai potensi penyalahgunaan aset kripto dalam aktivitas pencucian uang, meskipun hingga saat ini regulasi yang ketat terhadap penggunaan kripto masih dalam tahap pengembangan dan belum sepenuhnya diimplementasikan.[57]

Di sisi lain, lembaga perbankan dan jasa keuangan semakin menyadari pentingnya penerapan teknologi pencegahan, seperti sistem Know Your Customer (KYC) dan Anti Money Laundering (AML). KYC dan AML berfungsi untuk memverifikasi identitas nasabah serta memantau transaksi yang mencurigakan yang berpotensi berkaitan dengan TPPU atau TPPT. Di tingkat internasional, Uni Eropa melalui regulasi kelima Anti-Money Laundering Directive (5AMLD) mewajibkan transparansi data nasabah guna menekan praktik pencucian uang dan pendanaan terorisme.[58] Di Indonesia, OJK juga telah mewajibkan perbankan untuk memperkuat penerapan sistem KYC dan AML. Namun, tantangan tetap ada dalam pengawasan yang efektif, terutama terhadap transaksi yang menggunakan teknologi tinggi dan dilakukan secara lintas yurisdiksi.[59]

Penegakan hukum dan regulasi perlu mengikuti perkembangan teknologi dan modus kejahatan yang semakin kompleks seiring evolusi kejahatan perbankan. Kerja sama antarnegara dan antarinstansi menjadi kunci dalam menangani TPPU dan TPPT yang melibatkan teknologi canggih serta jaringan lintas negara. Sebagai contoh, kerja sama internasional antara Interpol, FATF, dan lembaga keuangan global memainkan peran penting dalam mengidentifikasi dan menangani jaringan kejahatan global yang memanfaatkan sistem perbankan sebagai sarana pencucian uang.[60] Bagi Indonesia, peningkatan kerja sama internasional dalam deteksi dan

[54] Fausto Martin De Sanctis, *International Money Laundering Through Real Estate and Agribusiness: A Criminal Justice Perspective from the "Panama Papers"* (Cham: Springer International Publishing, 2017), https://doi.org/10.1007/978-3-319-52069-8.

[55] Afriansyah, Ghozi, and Wargadalem, "Indonesia's Laws and Policies in Combatting Terrorism Financing"; Riswanto Riswanto et al., "Legal Aspects In Handling Money Laundering Cases In Indonesia," *Asian Journal of Social and Humanities* 2, no. 8 (2024): 1818–23, https://doi.org/10.59888/ajosh.v2i8.318.

[56] Samira Ibrahim et al., "Cybercrimeand Cryptocurrency," *American Journal of Engineering Research* 10, no. 12 (2021): 103–6.

[57] Meiryani, Soepriyanto, and Audrelia, "Effectiveness of Regulatory Technology Implementation in Indonesian Banking Sector to Prevent Money Laundering and Terrorist Financing."

[58] Joni Rönkkö, "Key Changes of the 5th EU AML Directive and Its Effects on the Finnish Banking Sector," LUT University, last modified 2022, https://lutpub.lut.fi/handle/10024/163950.

[59] Alina Bukhtiarova et al., "Assessment of Financial Monitoring Efficiency in the Banking System of Ukraine," *Banks and Bank Systems* 15, no. 1 (2023): 98–106.

[60] O. V. Prokopenko et al., "The Role of Banks in National Innovation System: General Strategical Analytics," *Financial and Credit Activity Problems of Theory and Practice* 3, no. 30 (2019): 26–35, https://doi.org/10.18371/fcaptp.v3i30.179455.

penanganan kejahatan keuangan sangat penting untuk memperkuat sistem keamanan perbankan nasional serta melindungi nasabah dari risiko kejahatan keuangan yang semakin kompleks.[61]

Upaya Pencegahan dan Penanggulangan Kejahatan Perbankan

Kebijakan dan regulasi pemerintah memainkan peran krusial dalam mencegah dan menangani kejahatan di sektor perbankan. Pemerintah dapat menetapkan standar keamanan yang ketat dan mengatur praktik perbankan guna menghindari celah yang dapat dimanfaatkan pelaku kejahatan. Undang-undang Anti Pencucian Uang (APU) dan regulasi perlindungan data pribadi, seperti General Data Protection Regulation (GDPR) di Uni Eropa, menyediakan kerangka hukum untuk memberantas kejahatan keuangan. Menurut Bukhtiarova dkk. (2023), efektivitas sistem pemantauan keuangan dalam sektor perbankan sangat bergantung pada penerapan regulasi yang ketat serta pengawasan yang berkelanjutan.[62] Regulasi yang komprehensif membantu dalam mengidentifikasi dan memitigasi risiko keuangan, serta mendorong lembaga keuangan untuk memperkuat praktik keamanannya.[63]

Lembaga perbankan juga menerapkan berbagai langkah preventif untuk melindungi diri dari kejahatan perbankan. Langkah-langkah ini meliputi penerapan kontrol akses yang ketat, audit internal secara berkala, dan sistem deteksi kecurangan (*fraud detection systems*). Menurut Suh dkk., pengurangan faktor risiko dan peluang terjadinya kecurangan merupakan strategi penting dalam meminimalkan insiden kejahatan di lembaga keuangan.[64] Selain itu, perbankan juga berinvestasi dalam pelatihan pegawai untuk meningkatkan kemampuan dalam mengenali dan menangani potensi ancaman. Abad-Segura dkk. mencatat bahwa integrasi teknologi keuangan (*fintech*) yang canggih dalam sistem perbankan dapat meningkatkan efisiensi operasional sekaligus memperkuat keamanan.[65]

Teknologi dan inovasi berperan penting dalam meningkatkan sistem keamanan perbankan. Penggunaan teknologi seperti *blockchain* dan kecerdasan buatan (*artificial intelligence*/AI) dapat memperkuat sistem pertahanan dan mengurangi risiko kejahatan. Demirkan dkk. menjelaskan bahwa teknologi *blockchain* dapat meningkatkan transparansi dan keamanan data, sementara AI mampu mendeteksi anomali dan aktivitas mencurigakan dengan lebih cepat.[66] Teknologi-teknologi ini mendukung upaya pencegahan kejahatan dengan menyediakan alat canggih untuk memantau serta mengamankan transaksi dan data nasabah.[67]

Pendidikan publik dan peningkatan kesadaran merupakan komponen kunci dalam upaya pencegahan kejahatan perbankan. Program edukasi bagi nasabah dan pegawai terkait risiko keamanan siber dan praktik perlindungan data dapat menurunkan kemungkinan terjadinya tindak kejahatan. Spoorthi dkk. (2024) menekankan pentingnya peningkatan kesadaran terhadap teknik *social engineering* dan *phishing* untuk melindungi individu maupun institusi

[61] Fany Dewi Rengganis and Dwi Setiawan Susanto, "Evaluation of the Anti-Money Laundering Programs Implementation in Indonesia," *Integritas: Jurnal Antikorupsi* 9, no. 2 (2023): 229–40, https://doi.org/10.32697/integritas.v9i2.973.

[62] Bukhtiarova et al., "Assessment of Financial Monitoring Efficiency in the Banking System of Ukraine."

[63] Prokopenko et al., "The Role of Banks in National Innovation System."

[64] Joon B. Suh, Rebecca Nicolaides, and Richard Trafford, "The Effects of Reducing Opportunity and Fraud Risk Factors on the Occurrence of Occupational Fraud in Financial Institutions," *International Journal of Law, Crime and Justice* 56 (2019): 79–88, https://doi.org/10.1016/j.ijlcj.2019.01.002.

[65] Emilio Abad-Segura et al., "Financial Technology: Review of Trends, Approaches and Management," *Mathematics* 8, no. 6 (2020): 951, https://doi.org/10.3390/math8060951..

[66] Sebahattin Demirkan, Irem Demirkan, and Andrew McKee, "Blockchain Technology in the Future of Business Cyber Security and Accounting," *Journal of Management Analytics* 7, no. 2 (2020): 189–208, https://doi.org/10.1080/23270012.2020.1731721.

[67] Broby, "Financial Technology and the Future of Banking"; Albert Tan, David Gligor, and Azizi Ngah, "Applying Blockchain for Halal Food Traceability," *International Journal of Logistics Research and Applications* 25, no. 6 (2022): 947–64, https://doi.org/10.1080/13675567.2020.1825653.

dari serangan siber.[68] Selain itu, Sahoo dan Kotiya menunjukkan bahwa pelatihan berkelanjutan dalam teknologi keamanan informasi dapat memperkuat ketahanan lembaga perbankan terhadap ancaman dunia maya.[69] Upaya pencegahan dan penanggulangan kejahatan perbankan memerlukan pendekatan multifaset yang mencakup kebijakan pemerintah, praktik internal lembaga perbankan, pemanfaatan teknologi canggih, dan edukasi publik. Kombinasi dari berbagai strategi ini dapat secara signifikan mengurangi risiko maupun dampak dari kejahatan perbankan.

Kasus-kasus kejahatan perbankan memberikan pelajaran berharga terkait pentingnya penerapan sistem keamanan yang komprehensif. Insiden seperti kebocoran data berskala besar menunjukkan kelemahan pada protokol keamanan yang ada, serta menegaskan urgensi untuk melakukan pembaruan teknologi secara berkala. Sebagai contoh, Demirkan dkk. menyoroti bahwa teknologi *blockchain* dapat memperkuat sistem keamanan perbankan melalui peningkatan transparansi dan pengurangan potensi penipuan (*fraud*).[70] Kesadaran ini mendorong lembaga perbankan untuk mengimplementasikan solusi teknologi terkini, seperti enkripsi data dan sistem deteksi kecurangan yang lebih canggih, guna melindungi informasi sensitif serta menekan risiko terjadinya serangan siber.

Pelajaran penting lainnya dari kasus kejahatan perbankan adalah perlunya integrasi yang ketat antara kebijakan dan praktik keamanan. Kasus-kasus penipuan besar seringkali mengungkap kesenjangan dalam regulasi yang berlaku atau kurangnya kepatuhan terhadap standar keamanan. Bukhtiarova dkk. (2023) mencatat bahwa efektivitas pengawasan keuangan sangat bergantung pada penerapan regulasi secara konsisten serta pengawasan yang ketat.[71] Oleh karena itu, lembaga perbankan harus berperan aktif dalam perumusan dan implementasi kebijakan keamanan, serta memastikan kepatuhan terhadap peraturan yang berlaku untuk mencegah terulangnya insiden serupa di masa depan.

Tabel 4. Analisis Peran Berbagai Aktor dalam Pencegahan Kejahatan Perbankan.

Aktor	Peran Utama	Tindakan Pencegahan & Mitigasi	Hasil yang Diharapkan
Nasabah	Pengguna akhir layanan perbankan	- Meningkatkan literasi digital dan keuangan - Menggunakan otentikasi dua faktor (2FA, OTP) - Melaporkan aktivitas mencurigakan	Peningkatan kesadaran dan ketahanan pribadi terhadap kejahatan siber
Bank	Penyedia layanan dan pengelola sistem keuangan	- Menerapkan teknologi keamanan tingkat lanjut (kecerdasan buatan/AI, biometrik, enkripsi) - Melakukan pemantauan transaksi secara real-time - Memberikan edukasi dan pelatihan kepada nasabah	Sistem keamanan internal yang kuat dan layanan perbankan yang aman

[68] Spoorthi et al., "Impacts of Social Engineering on E-Banking."

[69] Bhagyashree Sahoo and Minal Kotiya, "E-Banking: Innovation Challenges and Opportunities," *International Journal of Research in Engineering, Science and Management* 5, no. 5 (2022): 103–8.

[70] Demirkan, Demirkan, and McKee, "Blockchain Technology in the Future of Business Cyber Security and Accounting."

[71] Bukhtiarova et al., "Assessment of Financial Monitoring Efficiency in the Banking System of Ukraine."

Regulator	Pengawas dan pembuat kebijakan di sektor keuangan	- Menegakkan regulasi Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU/PPT) - Melakukan audit rutin dan pemeriksaan kepatuhan - Menyediakan sarana pelaporan publik (contoh: PPATK, GRIPS)	Kepatuhan regulasi yang tinggi dan deteksi dini terhadap aktivitas mencurigakan
Pemerintah	Pembuat kebijakan nasional dan penjaga kerangka hukum	- Menyelaraskan kebijakan nasional dan internasional - Memperkuat kapasitas aparat penegak hukum - Berinvestasi pada infrastruktur teknologi dan pengembangan sumber daya manusia	Stabilitas sistemik dan perlindungan hukum yang kuat bagi seluruh pemangku kepentingan

Sumber: Data olahan, 2024

Kasus kejahatan perbankan juga menekankan pentingnya pendidikan dan pelatihan berkelanjutan bagi pegawai dan nasabah guna menghadapi ancaman siber seperti *phishing* dan rekayasa sosial (*social engineering*), yang sering berhasil karena rendahnya tingkat kesadaran keamanan. Studi oleh Spoorthi dkk. (2024) menyoroti perlunya edukasi yang difokuskan pada pencegahan teknik *social engineering*, yang dapat mengurangi risiko kerentanan sistem perbankan terhadap serangan.[72] Dalam konteks Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT), pelatihan ini juga harus mencakup pemahaman terhadap indikator transaksi mencurigakan yang berpotensi terkait dengan pencucian uang atau pendanaan terorisme. Dengan demikian, peningkatan kapasitas pegawai dalam mendeteksi pola transaksi mencurigakan, serta koordinasi yang lebih baik dengan otoritas terkait, dapat memperkuat ketahanan sektor perbankan terhadap ancaman kejahatan siber dan TPPU/TPPT, sekaligus menjaga integritas sistem perbankan secara menyeluruh.

Strategi Pencegahan dan Penanganan TPPU dan TPPT dalam Sistem Perbankan Modern

Dalam menghadapi ancaman Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT), lembaga perbankan perlu menerapkan pendekatan komprehensif yang menggabungkan teknologi, regulasi, serta pemahaman mendalam terhadap risiko. Salah satu langkah awal dalam mencegah kejahatan keuangan ini adalah melalui penerapan sistem *Know Your Customer* (KYC), yang memungkinkan bank untuk melakukan verifikasi identitas nasabah secara lebih akurat dan mendeteksi transaksi mencurigakan sejak dini. KYC telah menjadi persyaratan standar di banyak negara dan terus disempurnakan seiring dengan berkembangnya modus kejahatan keuangan. Menurut Kandachamy, penerapan KYC yang ketat di Eropa terbukti efektif dalam menurunkan risiko pencucian uang, terutama melalui verifikasi data nasabah yang lebih akurat.[73] Di Indonesia, Otoritas Jasa Keuangan (OJK) mewajibkan seluruh bank untuk menerapkan KYC sebagai bagian dari strategi pencegahan TPPU dan TPPT.

Selain KYC, penerapan sistem Anti-Money Laundering (AML) yang efektif sangat penting untuk mengidentifikasi dan menghentikan aliran dana yang mencurigakan. Sistem AML bekerja dengan cara memantau transaksi yang tidak biasa atau mencurigakan yang dapat

[72] Spoorthi et al., "Impacts of Social Engineering on E-Banking."

[73] Archana Gokul Kandachamy, "Overview of Anti-Money Laundering in the Banking Industry : An Explanation of AML and the Importance of It in the Banking Sector," *Management and Quality* 5, no. 3 (2023): 79–89.

mengindikasikan adanya praktik pencucian uang atau pendanaan terorisme. Dalam penelitian yang dilakukan oleh Jiao dan Kumar dkk., integrasi teknologi dalam sistem AML—seperti *big data* dan *machine learning*—memungkinkan bank untuk menganalisis data transaksi secara real-time dan mendeteksi pola anomali yang sebelumnya sulit dikenali.[74] Dengan demikian, bank dapat merespons ancaman TPPU dan TPPT secara cepat, meminimalkan kerugian, dan memastikan transparansi operasional.

Penerapan teknologi *blockchain* juga mulai dipertimbangkan sebagai salah satu cara untuk melacak dan mengurangi risiko Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT). *Blockchain* menawarkan keamanan tambahan melalui pencatatan yang transparan dan sulit dimanipulasi. Dalam studi yang dilakukan oleh Dhanawat dan Javaid dkk., *blockchain* terbukti mampu menyediakan jalur pelacakan (*traceability*) transaksi yang kuat, sehingga memudahkan regulator dan lembaga keuangan dalam menelusuri aliran dana yang dicurigai terlibat dalam TPPU.[75] Beberapa negara, seperti Singapura, telah menerapkan teknologi *blockchain* dalam sektor perbankan sebagai bagian dari upaya pencegahan TPPU, dengan hasil menunjukkan peningkatan dalam deteksi aliran dana mencurigakan.

Di sisi regulasi, kolaborasi internasional dalam pencegahan TPPU dan TPPT semakin diperkuat melalui inisiatif seperti *Financial Action Task Force* (FATF), yang menetapkan standar global dalam memerangi pencucian uang dan pendanaan terorisme. FATF memberikan panduan bagi negara-negara untuk mengadopsi kerangka regulasi yang seragam, sehingga memungkinkan kerja sama lintas batas dalam menangani kejahatan keuangan internasional. Berdasarkan laporan FATF tahun 2021, negara-negara yang telah menerapkan standar FATF mengalami penurunan kasus TPPU dan TPPT, yang menunjukkan efektivitas kebijakan tersebut dalam mencegah kejahatan keuangan global.

Namun, penerapan kebijakan dan teknologi canggih ini juga menghadapi tantangan, khususnya dalam hal biaya, infrastruktur, dan kompetensi sumber daya manusia. Di Indonesia, tantangan ini sering dihadapi oleh bank-bank daerah yang memiliki keterbatasan dalam mengimplementasikan sistem *Anti-Money Laundering* (AML) atau teknologi *blockchain* karena keterbatasan dana. Zavoli dan King menyatakan bahwa hambatan-hambatan ini dapat diatasi melalui dukungan pemerintah serta peningkatan pelatihan bagi karyawan perbankan agar lebih kompeten dalam mengelola teknologi pencegahan kejahatan keuangan.[76] Dengan demikian, keberhasilan strategi pencegahan TPPU dan TPPT dalam sistem perbankan modern membutuhkan sinergi antara teknologi, regulasi, dan dukungan pemerintah yang berkelanjutan.

Salah satu kasus Tindak Pidana Pencucian Uang (TPPU) yang paling baru dan menonjol di Indonesia adalah kasus tahun 2023 yang terkait dengan transfer dana mencurigakan yang terhubung dengan jaringan perjudian daring ilegal. Menurut laporan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), dana dalam jumlah miliaran rupiah ditelusuri mengalir ke berbagai rekening yang menggunakan identitas palsu, sering kali melalui perantara pihak

[74] Mingyuan Jiao, "Big Data Analytics for Anti-Money Laundering Compliance in the Banking Industry," *Highlights in Science, Engineering and Technology* 49 (2023): 302–9, https://doi.org/10.54097/hset.v49i.8522; Ashwini Kumar et al., "Analysis of Classifier Algorithms to Detect Anti-Money Laundering," in *Computationally Intelligent Systems and Their Applications*, ed. Jagdish Chand Bansal et al. (Singapore: Springer, 2021), 143–52, https://doi.org/10.1007/978-981-16-0407-2_11.

[75] Vineet Dhanawat, "Anomaly Detection in Financial Transactions Using Machine Learning and Blockchain Technology," *International Journal of Business Management and Visuals* 5, no. 1 (2022): 34–41; Mohd Javaid et al., "A Review of Blockchain Technology Applications for Financial Services," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations* 2, no. 3 (2022): 100073, https://doi.org/10.1016/j.tbench.2022.100073.

[76] Ilaria Zavoli and Colin King, "The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis," *The Modern Law Review* 84, no. 4 (2021): 740–71, https://doi.org/10.1111/1468-2230.12628.

ketiga dan platform *fintech* untuk menyamarkan sumber serta tujuan dana. Kasus ini menunjukkan bagaimana layanan keuangan digital yang tidak diawasi secara ketat dapat dimanfaatkan untuk mencuci hasil kejahatan. Hal ini juga mencerminkan lemahnya proses verifikasi pada beberapa layanan perbankan digital dan dompet elektronik (*e-wallet*). Sebagai respons, otoritas Indonesia, termasuk Bank Indonesia dan Otoritas Jasa Keuangan (OJK), meningkatkan pengawasan regulasi dengan merevisi protokol *Know Your Customer* (KYC) dan *customer due diligence*, terutama pada sektor *fintech* dan lembaga *peer-to-peer lending*. Insiden ini menegaskan sifat ancaman TPPU yang terus berkembang dan memperkuat urgensi kolaborasi lintas sektor serta inovasi teknologi dalam penegakan sistem Anti-Pencucian Uang (APU).

Selain kasus perjudian daring ilegal, TPPU dalam sektor perbankan Indonesia juga memiliki kaitan erat dengan Pendanaan Terorisme (TPPT). Beberapa kasus pendanaan terorisme melalui transaksi perbankan terjadi dalam konteks pembiayaan aksi teror oleh kelompok teroris di Indonesia. Contohnya, sejumlah kelompok teroris lokal menggunakan rekening bank reguler untuk menerima donasi dari pihak-pihak tertentu, yang kemudian dananya digunakan untuk membiayai kegiatan terorisme. Berdasarkan data dari Badan Nasional Penanggulangan Terorisme (BNPT), ditemukan bahwa kelompok teroris kerap memanfaatkan celah dalam sistem pemantauan transaksi perbankan untuk menyamarkan asal-usul dana. Kondisi ini mendorong pemerintah Indonesia untuk memperketat pengawasan terhadap transaksi perbankan yang mencurigakan dan memperkuat kerja sama antara PPATK, BNPT, serta lembaga perbankan guna mencegah praktik pendanaan terorisme.

Kasus-kasus terbaru di Indonesia menunjukkan semakin kompleksnya risiko terkait TPPU dan TPPT di era digital. PPATK melaporkan adanya peningkatan kasus penipuan digital dan pencucian uang yang dipicu oleh inovasi dalam keuangan digital, seperti sistem pembayaran elektronik dan platform mata uang kripto. Fenomena ini menimbulkan kekhawatiran di kalangan lembaga keuangan karena alat digital tersebut memungkinkan praktik pencucian uang lintas negara tanpa deteksi langsung. Sebagai tanggapan, Indonesia telah memperkuat kerangka respons terhadap ancaman keuangan digital dengan memperketat regulasi terkait verifikasi identitas digital dan pemantauan transaksi. Selain itu, Indonesia juga memfokuskan upaya pemberantasan TPPT dengan meningkatkan koordinasi antarlembaga serta menjalin kerja sama erat dengan mitra internasional. Upaya terkini difokuskan pada pemantauan dana yang ditransfer melalui skema perdagangan dan memastikan bahwa organisasi non-profit (NPO) tidak disalahgunakan untuk membiayai terorisme. Meskipun langkah-langkah ini menunjukkan perkembangan positif, penyesuaian yang berkelanjutan tetap diperlukan untuk mengikuti perkembangan pesat teknologi keuangan dan taktik yang digunakan oleh kelompok kejahatan terorganisir.

Regulasi di Indonesia terkait Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT) telah mengalami perkembangan yang signifikan dalam beberapa tahun terakhir. Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan TPPU serta Undang-Undang No. 9 Tahun 2013 tentang Pencegahan dan Pemberantasan TPPT merupakan dasar hukum utama. Regulasi ini bertujuan untuk memperkuat upaya dalam mencegah, mendeteksi, dan menindak praktik pencucian uang dan pendanaan terorisme. Selain itu, Indonesia juga telah membentuk Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) sebagai lembaga yang memantau kepatuhan lembaga keuangan terhadap peraturan anti pencucian uang serta menerima dan menganalisis laporan transaksi keuangan mencurigakan yang dapat mengindikasikan TPPU atau TPPT.

Namun demikian, kelemahan utama dari regulasi ini terletak pada aspek implementasinya, khususnya dalam hal pengawasan yang ketat dan penerapan sanksi atas pelanggaran. Meskipun PPATK aktif dalam mengumpulkan data dan menyusun laporan transaksi mencurigakan, tantangan muncul dari terbatasnya sumber daya untuk melakukan penyelidikan mendalam

terhadap setiap laporan. Kelemahan lainnya adalah kesenjangan dalam kolaborasi internasional, di mana transaksi lintas negara sering kali sulit dilacak karena keterbatasan akses data atau perbedaan kerangka hukum antarnegara. Dalam konteks pendanaan terorisme, tantangan ini menjadi semakin kompleks karena melibatkan jaringan keuangan tersembunyi yang sulit ditelusuri.

Penelitian ini menawarkan beberapa rekomendasi untuk memperkuat regulasi dan pencegahan TPPU dan TPPT di Indonesia. Pertama, peningkatan kapasitas kelembagaan PPATK dan otoritas terkait menjadi hal yang sangat penting di era digital, di mana volume dan kompleksitas transaksi keuangan terus meningkat. Dengan semakin luasnya penggunaan sistem pembayaran digital seperti QRIS, modus penipuan pun turut berkembang, sering kali melibatkan kode *merchant* palsu atau tautan pembayaran yang menyesatkan yang disebarkan melalui *marketplace* daring seperti Shopee dan Tokopedia. Taktik ini membuat upaya pemantauan aktivitas mencurigakan menjadi lebih sulit tanpa alat deteksi yang canggih dan penyidik yang terlatih. Oleh karena itu, penguatan sumber daya kelembagaan, termasuk kapasitas sumber daya manusia dan infrastruktur teknologi, menjadi fondasi krusial dalam memperkuat ketahanan nasional terhadap kejahatan keuangan.

Kedua, pentingnya kerja sama internasional terletak pada sifat lintas batas dari kejahatan keuangan modern. Banyak kasus penipuan terbaru tidak hanya melibatkan pelaku domestik, tetapi juga jaringan internasional yang memanfaatkan sistem transaksi lintas negara untuk menyamarkan aliran dana ilegal. Misalnya, notifikasi pengiriman palsu yang mengatasnamakan layanan ekspedisi besar digunakan sebagai sarana untuk menipu pembayaran, yang kemudian dialirkan melalui platform pinjaman online atau dompet digital, dan dengan cepat ditransfer ke berbagai yurisdiksi. Tanpa adanya kerangka kerja yang komprehensif dan transparan untuk pertukaran informasi lintas negara, upaya pelacakan dana tersebut sering kali terhenti di batas yurisdiksi nasional. Oleh karena itu, keterlibatan aktif Indonesia dalam mekanisme global AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) akan sangat membantu dalam menutup kesenjangan penegakan hukum yang krusial.

Ketiga, peningkatan pelatihan dan kesadaran publik, khususnya di kalangan pegawai perbankan dan *fintech*, sangat penting untuk mengenali indikator transaksi mencurigakan. Semakin banyak kasus pencucian uang yang terkait dengan penyalahgunaan data pribadi dari pengajuan pinjaman online atau pembukaan rekening, di mana pelaku menggunakan identitas palsu untuk memanipulasi sistem. Pegawai garis depan sering kali menjadi pihak pertama yang menemui kejanggalan tersebut, namun tidak memiliki pelatihan memadai untuk menafsirkannya sebagai potensi ancaman. Peningkatan edukasi dan penerapan sistem peringatan dini akan memberdayakan lembaga keuangan untuk bertindak cepat dan melaporkan aktivitas mencurigakan. Ketiga strategi ini—penguatan kapasitas kelembagaan, kerja sama internasional, dan pelatihan proaktif sektor keuangan—membentuk pendekatan terintegrasi untuk menjaga ekosistem keuangan Indonesia dari ancaman TPPU dan TPPT yang terus berkembang.

Kesimpulan

Studi ini mengidentifikasi adanya pergeseran pola kejahatan dalam sistem perbankan, di mana kemajuan teknologi telah mentransformasi bentuk penipuan tradisional seperti pemalsuan cek dan kartu kredit menjadi bentuk kejahatan siber yang lebih canggih, termasuk *phishing*, *ransomware*, dan pelanggaran data (*data breach*). Kejahatan-kejahatan ini mencerminkan *modus operandi* yang terus berkembang, di mana para pelaku memanfaatkan kelemahan dalam infrastruktur digital dan sering kali berhasil menghindari mekanisme keamanan yang sudah usang. Studi ini juga menemukan bahwa kejahatan siber semakin terhubung erat dengan Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT), karena penggunaan platform digital internasional dan transaksi anonim dimanfaatkan untuk

menyamarkan asal-usul dan tujuan dana ilegal. Perkembangan ini menunjukkan adanya kerentanan tidak hanya dalam aspek teknis, tetapi juga dalam aspek regulasi dan kelembagaan, yang membutuhkan respon terkoordinasi.

Studi ini mengusulkan beberapa rekomendasi untuk menghadapi tantangan tersebut. Pertama, lembaga seperti PPATK perlu diperkuat dari segi sumber daya dan kapabilitas teknis, khususnya dalam memantau volume transaksi digital yang sangat besar. Kedua, sektor keuangan, termasuk perbankan dan *fintech*, perlu meningkatkan pengendalian internal melalui adopsi sistem berbasis kecerdasan buatan (AI) untuk deteksi anomali dan prediksi penipuan. Di saat yang sama, lembaga pengawas seperti OJK dan Bank Indonesia harus menerapkan regulasi yang adaptif dan proaktif, yang selaras dengan laju inovasi digital. Ketiga, pada tingkat industri, mekanisme kerja sama internasional sangat diperlukan untuk melacak aliran dana lintas negara, terutama yang dicurigai berkaitan dengan TPPU dan TPPT. Terakhir, program pendidikan dan pelatihan komprehensif harus diberikan tidak hanya kepada pegawai garis depan, tetapi juga kepada nasabah bank dan pengguna layanan *fintech*. Langkah ini penting untuk meningkatkan literasi digital, memperkuat kesadaran terhadap ancaman, serta mempercepat respons kelembagaan terhadap aktivitas mencurigakan. Dengan menerapkan langkah-langkah ini, para pemangku kepentingan di semua level dapat membangun lingkungan perbankan digital di Indonesia yang lebih tangguh, transparan, dan aman.

Daftar Pustaka

Abad-Segura, Emilio, Mariana-Daniela González-Zamar, Eloy López-Meneses, and Esteban Vázquez-Cano. "Financial Technology: Review of Trends, Approaches and Management." *Mathematics* 8, no. 6 (2020): 951. https://doi.org/10.3390/math8060951.

Achim, Monica Violeta, and Sorin Nicolae Borlea. *Economic and Financial Crime: Corruption, Shadow Economy, and Money Laundering*. Vol. 20. Studies of Organized Crime. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-51780-9.

Afriansyah, Arie, Ahmad Ghozi, and M Akila Wargadalem. "Indonesia's Laws and Policies in Combatting Terrorism Financing: An Update Analysis." *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2, no. 1 (2023): 1–18. https://doi.org/10.59593/amlcft.2023.v2i1.49.

Ali, Shazeeda. "Criminal Minds: Profiling Architects of Financial Crimes." *Journal of Financial Crime* 28, no. 2 (2021): 324–44. https://doi.org/10.1108/JFC-11-2020-0221.

Alzoubi, Haitham M., Taher M. Ghazal, Mohammad Kamrul Hasan, Asma Alketbi, Rukshanda Kamran, Nidal A. Al-Dmour, and Shayla Islam. "Cyber Security Threats on Digital Banking." In *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 1–4. IEEE, 2022. https://ieeexplore.ieee.org/abstract/document/9896966/.

Azernikov, A. D., A. N. Norkina, E. R. Myseva, and K. A. Chicherov. "Innovative Technologies in Combating Cyber Crime." *KnE Social Sciences* 3, no. 2 (2018): 248–52. https://doi.org/10.18502/kss.v3i2.1550.

Broby, Daniel. "Financial Technology and the Future of Banking." *Financial Innovation* 7, no. 1 (2021): 47. https://doi.org/10.1186/s40854-021-00264-y.

Bukhtiarova, Alina, Andrii Semenog, Mila Razinkova, Nataliia Nebaba, and Józef Antoni Haber. "Assessment of Financial Monitoring Efficiency in the Banking System of Ukraine." *Banks and Bank Systems* 15, no. 1 (2023): 98–106.

Burnes, David, Marguerite DeLiema, and Lynn Langton. "Risk and Protective Factors of Identity Theft Victimization in the United States." *Preventive Medicine Reports* 17 (2020): 101058. https://doi.org/10.1016/j.pmedr.2020.101058.

Choi, Kwan, Ju-lak Lee, and Yong-tae Chun. "Voice Phishing Fraud and Its Modus Operandi." *Security Journal* 30, no. 2 (2017): 454–66. https://doi.org/10.1057/sj.2014.49.

De Sanctis, Fausto Martin. *International Money Laundering Through Real Estate and Agribusiness: A Criminal Justice Perspective from the "Panama Papers."* Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-52069-8.

Demirkan, Sebahattin, Irem Demirkan, and Andrew McKee. "Blockchain Technology in the Future of Business Cyber Security and Accounting." *Journal of Management Analytics* 7, no. 2 (2020): 189–208. https://doi.org/10.1080/23270012.2020.1731721.

Dhanawat, Vineet. "Anomaly Detection in Financial Transactions Using Machine Learning and Blockchain Technology." *International Journal of Business Management and Visuals* 5, no. 1 (2022): 34–41.

Driel, Hugo van. "Financial Fraud, Scandals, and Regulation: A Conceptual Framework and Literature Review." *Business History* 61, no. 8 (2019): 1259–99. https://doi.org/10.1080/00076791.2018.1519026.

Fahlevi, Mochammad, Mohamad Saparudin, Sari Maemunah, Dasih Irma, and Muhamad Ekhsan. "Cybercrime Business Digital in Indonesia." *E3S Web of Conferences* 125 (2019): 21001. https://doi.org/10.1051/e3sconf/201912521001.

Ghelani, Diptiben, Tan Kian Hua, and Surendra Kumar Reddy Koduru. "Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking." *American Journal of Computer Science and Technology* (2022): 1–8. https://doi.org/10.22541/au.166385206.63311335/v1.

Gomes, Vanessa, Joaquim Reis, and Bráulio Alturas. "Social Engineering and the Dangers of Phishing." In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–7. IEEE, 2020. https://ieeexplore.ieee.org/abstract/document/9140445/.

Hasham, Salim, Shoan Joshi, and Daniel Mikkelsen. *Financial Crime and Fraud in the Age of Cybersecurity*. New Yok: McKinsey & Company, 2019.

Hashim, Hafiza Aishah, Zalailah Salleh, Izzati Shuhaimi, and Nurul Ain Najwa Ismail. "The Risk of Financial Fraud: A Management Perspective." *Journal of Financial Crime* 27, no. 4 (2020): 1143–59. https://doi.org/10.1108/JFC-04-2020-0062.

Hilal, Waleed, S. Andrew Gadsden, and John Yawney. "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances." *Expert Systems with Applications* 193 (2022): 116429. https://doi.org/10.1016/j.eswa.2021.116429.

Ibrahim, Samira, Daniel Ikechukwu Nnamani, Ojeifoh Okosun, and Olumuyiwa Ezekiel Soyele. "Cybercrimeand Cryptocurrency." *American Journal of Engineering Research* 10, no. 12 (2021): 103–6.

Imran, Mohammad Fadil. "Preventing and Combating Cybercrime in Indonesia." *International Journal of Cyber Criminology* 17, no. 1 (2023): 223–35.

Jakšič, Marko, and Matej Marinč. "Relationship Banking and Information Technology: The Role of Artificial Intelligence and FinTech." *Risk Management* 21, no. 1 (2019): 1–18. https://doi.org/10.1057/s41283-018-0039-y.

Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, and Shahbaz Khan. "A Review of Blockchain Technology Applications for Financial Services." *BenchCouncil Transactions on Benchmarks, Standards and Evaluations* 2, no. 3 (2022): 100073. https://doi.org/10.1016/j.tbench.2022.100073.

Jiao, Mingyuan. "Big Data Analytics for Anti-Money Laundering Compliance in the Banking Industry." *Highlights in Science, Engineering and Technology* 49 (2023): 302–9. https://doi.org/10.54097/hset.v49i.8522.

Kandachamy, Archana Gokul. "Overview of Anti-Money Laundering in the Banking Industry: An Explanation of AML and the Importance of It in the Banking Sector." *Management and Quality* 5, no. 3 (2023): 79–89.

Karpoff, Jonathan M. "The Future of Financial Fraud." *Journal of Corporate Finance* 66 (February 2021): 101694. https://doi.org/10.1016/j.jcorpfin.2020.101694.

Kumar, Ashwini, Sanjoy Das, Vishu Tyagi, Rabindra Nath Shaw, and Ankush Ghosh. "Analysis of Classifier Algorithms to Detect Anti-Money Laundering." In *Computationally Intelligent Systems and Their Applications*, edited by Jagdish Chand Bansal, Marcin Paprzycki, Monica Bianchini, and Sanjoy Das, 143–52. Singapore: Springer, 2021. https://doi.org/10.1007/978-981-16-0407-2_11.

Leo, Martin, Suneel Sharma, and K. Maddulety. "Machine Learning in Banking Risk Management: A Literature Review." *Risks* 7, no. 1 (2019): 29. https://doi.org/10.3390/risks7010029.

Lokanan, Mark. "Theorizing Financial Crimes as Moral Actions." *European Accounting Review* 27, no. 5 (2018): 901–38. https://doi.org/10.1080/09638180.2017.1417144.

Masciandaro, Donato. *Global Financial Crime: Terrorism, Money Laundering and Offshore Centres*. New York: Taylor & Francis, 2017.

Meiryani, Meiryani, Gatot Soepriyanto, and Jessica Audrelia. "Effectiveness of Regulatory Technology Implementation in Indonesian Banking Sector to Prevent Money Laundering and Terrorist Financing." *Journal of Money Laundering Control* 26, no. 4 (2022): 892–908. https://doi.org/10.1108/JMLC-04-2022-0059.

Mosteanu, Narcisa Roxana, and Alessio Faccia. "Digital Systems and New Challenges of Financial Management – FinTech, XBRL, Blockchain and Cryptocurrencies." *Quality – Access to Success* 21, no. 174 (2020): 159–66.

Navaretti, Giorgio Barba, Giacomo Calzolari, José Manuel Mansilla-Fernandez, and Alberto F. Pozzolo. "Fintech and Banking. Friends or Foes?" *Friends or Foes* (2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099337.

Nicholls, Jack, Aditya Kuppa, and Nhien-An Le-Khac. "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape." *Ieee Access* 9 (2021): 163965–86.

Payne, Brian K. "Defining Cybercrime." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited by Thomas J. Holt and Adam M. Bossler, 3–25. Cham: Palgrave Macmillan, 2020. https://doi.org/10.1007/978-3-319-78440-3_1.

Pospisil, Bettina, Edith Huber, Gerald Quirchmayr, and Walter Seboeck. "Modus Operandi in Cybercrime." In *Encyclopedia of Criminal Activities and the Deep Web*, 193–209. IGI Global Scientific Publishing, 2020. https://doi.org/10.4018/978-1-5225-9715-5.ch013.

Pratama, Yoga, Krisna Indra Sakti, Firmawan Setyadi, Nur Ahmad Azi Ibrahim, and Ali Mukti Nur Hidayat. "Cybercrime: The Phenomenon of Crime through the Internet in Indonesia." *Proceeding International Conference Restructuring and Transforming Law* 1, no. 1 (2022): 294–301.

Prokopenko, O. V., N. V. Biloshkurska, M. V. Biloshkurskyi, and V. A. Omelyanenko. "The Role of Banks in National Innovation System: General Strategical Analytics." *Financial and Credit Activity Problems of Theory and Practice* 3, no. 30 (2019): 26–35. https://doi.org/10.18371/fcaptp.v3i30.179455.

Reichman, Nancy. "Managing Crime Risks: Toward an Insurance Based Model of Social Control." In *Risk Management*, edited by Gerald Mars and David T. H. Weir, 45–66. London: Routledge, 2020.

Rengganis, Fany Dewi, and Dwi Setiawan Susanto. "Evaluation of the Anti-Money Laundering Programs Implementation in Indonesia." *Integritas: Jurnal Antikorupsi* 9, no. 2 (2023): 229–40. https://doi.org/10.32697/integritas.v9i2.973.

Riswanto, Riswanto, Muhammad Akbar Rachmatullah, Alip Rahman, and Diky Dikrurahman. "Legal Aspects In Handling Money Laundering Cases In Indonesia." *Asian Journal of Social and Humanities* 2, no. 8 (2024): 1818–23. https://doi.org/10.59888/ajosh.v2i8.318.

Rönkkö, Joni. "Key Changes of the 5th EU AML Directive and Its Effects on the Finnish Banking Sector." LUT University. Last modified 2022. https://lutpub.lut.fi/handle/10024/163950.

Sahoo, Bhagyashree, and Minal Kotiya. "E-Banking: Innovation Challenges and Opportunities." *International Journal of Research in Engineering, Science and Management* 5, no. 5 (2022): 103–8.

Spoorthi, M., H. L. Gururaj, V. Ambika, V. Janhavi, and H. Najmusher. "Impacts of Social Engineering on E-Banking." In *Social Engineering in Cybersecurity*, edited by H. L. Gururaj, V. Janhavi, and V. Ambika. Boca Raton: CRC Press, 2024.

Suh, Joon B., Rebecca Nicolaides, and Richard Trafford. "The Effects of Reducing Opportunity and Fraud Risk Factors on the Occurrence of Occupational Fraud in Financial Institutions." *International Journal of Law, Crime and Justice* 56 (2019): 79–88. https://doi.org/10.1016/j.ijlcj.2019.01.002.

Tan, Albert, David Gligor, and Azizi Ngah. "Applying Blockchain for Halal Food Traceability." *International Journal of Logistics Research and Applications* 25, no. 6 (2022): 947–64. https://doi.org/10.1080/13675567.2020.1825653.

Trozze, Arianna, Josh Kamps, Eray Arda Akartuna, Florian J. Hetzel, Bennett Kleinberg, Toby Davies, and Shane D. Johnson. "Cryptocurrencies and Future Financial Crime." *Crime Science* 11, no. 1 (2022): 1. https://doi.org/10.1186/s40163-021-00163-8.

Van Nguyen, Trong. "The Modus Operandi of Transnational Computer Fraud: A Crime Script Analysis in Vietnam." *Trends in Organized Crime* 25, no. 2 (2022): 226–47. https://doi.org/10.1007/s12117-021-09422-1.

Wewege, Luigi, Jeo Lee, and Michael C. Thomsett. "Disruptions and Digital Banking Trends." *Journal of Applied Finance & Banking* 10, no. 6 (2020): 15–56.

Zavoli, Ilaria, and Colin King. "The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis." *The Modern Law Review* 84, no. 4 (2021): 740–71. https://doi.org/10.1111/1468-2230.12628.