

Optimalisasi *Open Banking* pada Layanan Keuangan Digital dalam Penegakan Rezim Anti Pencucian Uang

Ganda Raharja Rusli, Anestia Hayubriandini Fermay*

PT Allo Bank Indonesia Tbk, Indonesia

*Korespondensi penulis: anestia.fermay@allobank.com

Kata Kunci:

Anti pencucian uang,
Layanan keuangan digital,
Open banking, *RegTech*

Abstrak

Teknologi telah merevolusi sistem keuangan, tetapi layanan yang mudah dan mulus meningkatkan risiko penipuan. Seiring pertumbuhan keuangan digital, sistem anti pencucian uang (*Anti-Money Laundering* – AML) menghadapi kesulitan dengan volume transaksi yang tinggi. Tujuan utama dari studi ini adalah untuk memverifikasi apakah *open banking* dapat menjadi katalis efisiensi pemantauan transaksi dalam AML. Tujuan lainnya adalah untuk menganalisis agenda saat ini dari regulator di Indonesia, yang terkait dengan Blueprint Sistem Pembayaran Indonesia (BSPI) 2025 dan keamanan data pelanggan. Teknik Delphi mengidentifikasi teknologi yang memenuhi peraturan anti pencucian uang kontemporer, yang mencakup pencucian uang, teknologi regulasi (*Regulatory Technology* – *RegTech*), dan regulator. Artikel ini mendalami analisis komparatif antara teknologi regulasi dan kejahatan keuangan, yang menekankan beberapa tindakan untuk memberantas pencucian uang, seperti memperkuat sistem AML, penyaringan pelanggan, dan memungkinkan berbagi data lintas lembaga. Selain itu, tulisan ini mengeksplorasi keterbatasan dan hambatan mendatang dari *RegTech* terkait kepatuhan AML. Temuan menunjukkan bahwa *open banking* menjadi katalis efisiensi pemantauan transaksi dalam AML dan mendukung agenda regulator untuk memerangi pencucian uang dengan beberapa persyaratan.

Dikirimkan: 28 Oktober 2023

Diterima: 31 Mei 2024

Diterbitkan: 1 Juni 2024

Copyright (c) Authors



Untuk mensitasi artikel ini: Rusli, G. R. & Fermay, A. H. 2024. *Optimalisasi Open Banking pada Layanan Keuangan Digital dalam Penegakan Rezim Anti Pencucian Uang*. *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2(2):159-174, <https://doi.org/10.59593/amlcft.2024.v2i2.158>

Pendahuluan

Menghubungkan perbankan dan teknologi keuangan (*FinTech*) melalui interkoneksi kedua layanan ini memungkinkan pelaku usaha kecil untuk melakukan transaksi bisnis dengan lebih mudah. Misalnya, dengan memberikan dukungan akses ke modal dan penyediaan sistem pembayaran yang aman serta mendorong pertumbuhan ekonomi.¹ Namun, terdapat masalah terkait pelacakan aliran transaksi pelanggan yang dicurigai terlibat dalam transaksi yang terkait dengan pencucian uang. Lembaga keuangan tidak memiliki wewenang untuk mengakses data jejak aktivitas keuangan konsumen yang sama di lembaga keuangan yang berbeda. Ketika dana pelanggan telah keluar ke lembaga keuangan lain, tidak akan mudah untuk mendapatkan gambaran

¹ (Bank Indonesia, 2019)

besar dari transaksi yang dilakukan oleh pelanggan tersebut. Oleh karena itu, berbagi data lintas lembaga melalui *open banking* diyakini sebagai solusi untuk menegakkan upaya anti pencucian uang (*Anti-Money Laundering*, selanjutnya disebut sebagai AML) di lembaga keuangan.

Teknologi dalam konteks ini merujuk pada alat dan sistem yang dirancang untuk mengefisiensi dan mengotomatisasi layanan keuangan. Pada dasarnya, layanan keuangan digital adalah solusi inovatif dalam layanan keuangan yang mencakup uang elektronik, *platform crowdfunding*, dan mata uang virtual. Komisi Eropa (2019)² telah mengidentifikasi sektor dan produk yang mungkin rentan terhadap risiko pencucian uang, termasuk transaksi tunai, sektor keuangan, industri perjudian, bisnis non-keuangan dan produknya, transfer dana yang dilakukan oleh organisasi nirlaba, dan beberapa sektor baru dengan produk unik. Memerangi kejahatan keuangan memerlukan kolaborasi antara regulator yang harus bekerja secara efisien bersama-sama.

Lembaga Keuangan memerlukan solusi *Regulatory Technology (RegTech)* untuk meningkatkan kepatuhan AML³ dan kemampuan pemantauan transaksi,⁴ serta memahami bagaimana cara terbaik untuk mengintegrasikan *RegTech* ke dalam operasi mereka.⁵ Komponen tertentu dari analisis sebelumnya menimbulkan pertanyaan tentang peran berbagi data dalam upaya Anti Pencucian Uang dan Pemberantasan Pendanaan Terorisme (*Anti-money Laundering and Counter-terrorism Financing - AML/CFT*). Akibatnya, model kerja sama antara pemerintahan dan lembaga keuangan telah dikembangkan di mana lembaga-lembaga ini berbagi data untuk tujuan AML/CFT, tetapi hal ini tidak akan mungkin terjadi tanpa pengembangan *RegTech*.⁶ Aliansi antara lembaga keuangan dan perusahaan teknologi⁷ atau pemangku kepentingan publik dan swasta⁸ sangat penting untuk perkembangan tersebut.

Pemerintah menetapkan kebijakan berbagi data melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)⁹ di mana berbagi data lintas lembaga diperbolehkan, sebagaimana tertulis dalam Pasal 15 ayat 1 (poin d, klausul tentang kepentingan pengawasan sektor jasa keuangan). Disebutkan bahwa hak-hak subjek data pribadi, sebagaimana dimaksud dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, dan Pasal 13 ayat (1) dan (2), dikecualikan dari pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka administrasi negara. UU PDP juga mendukung agenda Bank Indonesia terkait *Blueprint Sistem Pembayaran Indonesia 2025 (BSPI 2025)*.¹⁰

² European Commission, "Report from the Commission to the European Parliament and the Council," *Angewandte Chemie International Edition*, 6(11), (2019): 951–952, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0370&from=GA>.

³ Dirk A. Zetzsche et al., "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation," *SSRN Electronic Journal*, January (2017), <https://doi.org/10.2139/ssrn.3018534>.

⁴ Dionysios S. Demetis, "Fighting Money Laundering with Technology: A Case Study of Bank X in the UK," *Decision Support Systems* 105 (2018): 96–107, <https://doi.org/10.1016/j.dss.2017.11.005>.

⁵ Emily Lee, "Financial Inclusion: A Challenge to the New Paradigm of Financial Technology, Regulatory Technology and Anti-Money Laundering Law," *SSRN Electronic Journal*, (2018): 1–51, <https://doi.org/10.2139/ssrn.3018960>.

⁶ Douglas W. Arner, János Barberis, and Ross P. Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation," *Northwestern Journal of International Law and Business* 37, no. 3 (2017): 373–415; Dong Yang and Min Li, "Evolutionary Approaches and the Construction of Technology-Driven Regulations," *Emerging Markets Finance and Trade* 54, no. 14 (2018): 3256–71, <https://doi.org/10.1080/1540496X.2018.1496422>.

⁷ R. Butler, T. and Brooks, "On the Role of Ontology-Based RegTech for Managing Risk and Compliance Reporting in the Age of Regulation," *Journal of Risk Management in Financial Institutions* 11, no. 1 (2017): 19–33.

⁸ K. Lai, "Blockchain as AML Tool: A Work in Progress," *International Financial Law Review*, London, 2018.

⁹ 27th, 2022 on Personal Data Protection (UU PDP), <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022> accessed on August 6, 2023.

¹⁰ Indonesia Payment System Blueprint 2025, <https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx> accessed on July 22, 2023.

Blueprint tersebut terdiri dari lima visi sistem pembayaran menuju 2025 untuk diimplementasikan oleh lima kelompok kerja, yaitu *Open Banking*; Sistem Pembayaran Ritel; Sistem Pembayaran Bernilai Besar (*Wholesale*) dan Infrastruktur Pasar Keuangan; Data dan Digitalisasi; serta Reformasi Regulasi, Perizinan dan Pengawasan. BSPI 2025 memastikan keseimbangan inovasi melalui Implementasi Prinsip Mengenal Nasabah atau *Know Your Customer* (KYC) dan AML/CTF.

Tulisan ini bertujuan untuk memastikan bagaimana *open banking* meningkatkan efisiensi pemantauan transaksi dalam AML, serta memeriksa agenda regulasi Indonesia saat ini tentang BSPI 2025 dan keamanan data pelanggan. Dibandingkan dengan studi sebelumnya yang dilakukan oleh Arner *et al.* (2017) yang menggunakan regulator dan pembuat kebijakan sebagai subjek survei, studi ini berfokus pada pemangku kepentingan khusus yang merupakan ahli Kepatuhan AML dengan pengalaman intensif di industri keuangan dan perbankan selama lebih dari lima tahun.

Studi ini berpusat pada fakta dan kemajuan kontemporer, serta temuan tentang kasus-kasus kejahatan keuangan, khususnya yang menekankan pada ancaman pencucian uang. Selain itu, studi ini menjelaskan *RegTech* dan relevansinya dengan berbagi data lintas lembaga terkait *open banking*. Selanjutnya, penelitian tentang kemunculan teknologi baru di sektor keuangan dan perbankan, khususnya *FinTech* dan *RegTech*, telah memfasilitasi pemahaman yang lebih dalam tentang bagaimana inovasi memungkinkan lembaga keuangan mengembangkan solusi canggih. Mengelola data dengan baik menjadi semakin krusial karena merupakan sumber daya yang berharga untuk kemajuan ini. Akhirnya, studi ini mengusulkan rekomendasi tentang teknologi yang akan memainkan peran utama dalam pemantauan transaksi AML dengan mengoptimalkan *open banking*.

Metode Delphi digunakan untuk mengidentifikasi teknologi terbaru untuk kepatuhan AML, termasuk pencucian uang, *RegTech*, dan regulator. Studi ini membahas perbandingan antara *RegTech* dan kejahatan keuangan serta kendala dan tantangan masa depan *RegTech* untuk kepatuhan AML. Penelitian ini bersifat eksploratif menggunakan metode Delphi yang pada dasarnya dikembangkan oleh RAND Corporation (RAND, 2019).¹¹ Metodologi ini mengandalkan wawasan para ahli yang merespons serangkaian survei berulang untuk memperkirakan dan mengantisipasi tren yang akan datang dalam industri atau topik tertentu. Metode Delphi digunakan untuk menentukan empat tujuan utama dalam penelitian ini, yaitu:

1. Merekrut minimal enam ahli dalam kepatuhan AML dan *RegTech* yang terlibat atau bekerja di lembaga keuangan untuk menangani masalah anti-pencucian uang.
2. Menentukan elemen-elemen yang dominan, yang secara konsisten ditekankan oleh para ahli kepatuhan AML saat menggunakan *RegTech* dan teknologi canggih lainnya.
3. Mengalihkan fokus pada implikasi masa depan dari implementasi *RegTech* terhadap evolusi pencucian uang dalam jangka menengah hingga panjang.
4. Berupaya mencapai kesepakatan komprehensif (yang juga disebut "*konsensus*") di antara para ahli kepatuhan AML dan *RegTech* mengenai serangkaian tindakan yang dianggap sebagai tujuan penting oleh badan pengatur dalam memerangi kejahatan keuangan.

Setidaknya enam ahli harus direkrut untuk membuat penelitian ini relevan. Pada akhir proses perekrutan, enam profesional kepatuhan AML atau *RegTech* mengonfirmasi bahwa mereka dapat berpartisipasi dalam studi ini dan menjadi bagian dari panel ahli. Menurut penelitian,¹² setidaknya lima panel diperlukan untuk memastikan hasil yang realistis. Oleh karena itu, perekrutan enam spesialis dianggap cukup meskipun awalnya menghubungi lebih dari sepuluh ahli. Tujuannya adalah untuk menjaga ukuran panel yang relatif kecil untuk menjamin tingkat respons dan retensi

¹¹ Delphi method, www.rand.org/topics/delphi-method.html.

¹² Esman Kurum, "RegTech Solutions and AML Compliance: What Future for Financial Crime?," *Journal of Financial Crime* 30, no. 3 (2023): 776–94, <https://doi.org/10.1108/JFC-04-2020-0051>.

yang tinggi karena survei Delphi memerlukan komitmen peserta yang kuat. *Google Forms* digunakan sebagai alat pengumpulan data.

Survei terdiri dari dua fase, masing-masing cukup untuk mendapatkan konsensus di antara ahli yang disurvei. Jika tidak, fase ketiga dengan survei tambahan akan diperlukan. Fase pertama (disebut "*Fase 1*") mencakup pertanyaan terbuka dan luas tentang relevansi *RegTech* untuk kepatuhan AML dengan jawaban singkat, sedangkan Fase kedua (disebut "*Fase 2*") mencakup pertanyaan pilihan ganda yang lebih teknis dan disusun menggunakan hasil dari survei pertama. Oleh karena itu, data yang dikumpulkan bersifat kualitatif dan kuantitatif.

Para peserta, yang semuanya ahli atau memiliki pengalaman yang cukup dalam kepatuhan AML atau solusi *RegTech* dalam layanan keuangan digital, direkrut melalui pesan di Gmail. Makalah dan tautan web dikirimkan ke setiap peserta pada setiap fase melalui email untuk mengakses survei, dan pengingat dikirim melalui email kepada yang tidak merespons. Responden dan para ahli diberikan waktu dua minggu untuk mengisi survei pada tiap fase. Fase 1 dimulai pada 5–19 Agustus 2023, dan Fase 2 pada 20 Agustus–5 September 2023.

Eksplorasi Teknologi dalam Layanan Keuangan Digital

Bank Federal Reserve St. Louis melaporkan bahwa penipuan perbankan digital meningkat selama pandemi COVID-19.¹³ Selain itu, laporan dari *Business Insider Intelligence* menemukan bahwa penipuan pengambilalihan akun (ketika peretas mendapatkan akses tidak sah ke akun) telah meningkat lebih dari 280% sejak 2015.¹⁴ Eskalasi penipuan perbankan digital ini dapat didistribusikan pada lima faktor utama, yaitu:

1. Kemajuan teknologi, seperti sistem pembayaran digital (contohnya QRIS) telah membuat transaksi *online* lebih mudah diakses dan nyaman. Namun, ini juga menghadirkan ancaman baru, seperti kode QRIS palsu. Kode QRIS yang dihasilkan oleh pelaku kejahatan dapat mengarahkan korban ke halaman web penipuan yang meniru portal *login* asli untuk perbankan digital atau *platform* media sosial.
2. Keamanan siber yang lemah atau kurangnya protokol autentikasi yang kuat menyebabkan beberapa sistem perbankan digital terus bergantung pada protokol autentikasi kata sandi atau PIN yang rentan terhadap serangan *brute-force* dan strategi rekayasa sosial. Akibatnya, lembaga keuangan harus mengalokasikan sumber daya untuk menerapkan teknik autentikasi yang lebih kuat, seperti autentikasi biometrik dan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan sistem perbankan *online* mereka.
3. Kurangnya kepatuhan terhadap regulasi, seperti prosedur identifikasi dan verifikasi pelanggan yang tidak memadai, membuka pintu bagi penipu untuk membuka akun menggunakan identitas palsu atau informasi yang dicuri. Kelemahan dalam protokol keamanan, seperti langkah-langkah autentikasi yang tidak memadai, juga dapat menyebabkan akses tidak sah ke akun pelanggan. Selain itu, kurangnya pengawasan regulasi atau kegagalan untuk mematuhi regulasi dapat mengakibatkan kerentanan yang dieksploitasi oleh penipu.
4. Meningkatnya kecanggihan penipu yang menggunakan *machine-learning* dan kecerdasan buatan. Salah satu teknik yang digunakan adalah Pemrosesan Bahasa Alami (*Natural Language Processing* - NLP). Dengan teknik NLP, penipu memanfaatkan *chatbot* untuk berkomunikasi dengan pelanggan bank dan menyelundupkan uang. Teknik lainnya adalah Jaringan Adversarial Generatif (*Generative Adversarial Networks* - GANs), yang digunakan penipu untuk menghasilkan data sintesis seperti akun bank yang mirip dengan yang asli untuk tidak menimbulkan kecurigaan dari badan pengatur.

¹³<https://www.stlouisfed.org/on-the-economy/2022/sep/fed-guidelines-master-account-access-payment-services> accessed on July 22, 2023.

¹⁴<https://www.businessinsider.com/capitol-one-data-breach-has-heavy-implications-2019-7> accessed on July 22, 2023.

5. Ancaman internal, seperti kelalaian karyawan, pelanggaran karyawan, dan risiko pihak ketiga berkontribusi pada ancaman internal yang dihadapi lembaga keuangan jika tidak diaudit secara teratur dan tidak menerapkan kontrol internal yang ketat.

Terdapat korelasi yang kuat antara penipuan dan pencucian uang. Penipuan sering kali melibatkan perolehan dana secara ilegal, yang kemudian dicuci melalui berbagai cara untuk menyembunyikan asal-usulnya yang tidak sah. Dalam konteks ini, penipuan dan pencucian uang adalah dua sisi dari mata uang yang sama; dengan yang satu sering kali mengarah ke atau memfasilitasi yang lain. Dedikasi teguh Pemerintah Indonesia dalam memerangi pencucian uang telah dibuktikan melalui hasil Keputusan Mahkamah Konstitusi Nomor 15/PUU-XIX/2021 tentang hasil uji materiil Pasal 74 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (Undang-Undang Pencucian Uang) yang telah memberikan kepastian hukum dan memastikan keseragaman dalam interpretasi dan penegakan regulasi anti-pencucian uang.

Berbicara tentang eksploitasi teknologi dalam layanan keuangan digital dapat dilihat dalam beberapa kasus, seperti cabang Estonian dari Danske Bank, di mana miliaran Euro dicuci melalui akun non-residen. Contoh lainnya adalah kasus ABLV Bank di Latvia, yang dituduh oleh otoritas AS memfasilitasi aktivitas kriminal skala besar dan menjadi subjek sanksi.

Kasus lain termasuk investigasi terhadap potensi aktivitas pencucian uang di bank *online* Jerman N26 dan Revolut yang berbasis di Inggris. Pada tahun 2021, N26 dikenakan denda karena kelemahan dalam kontrol anti-pencucian uang dan menerima peringatan lain dari regulator keuangan Jerman, BaFin. Hal ini terjadi karena kekurangan dalam sistem AML-nya. Sementara itu, Revolut, yang dikenal sebagai "*aplikasi super keuangan tanpa batas*", menawarkan banyak layanan yang biasa dikaitkan dengan bank. Kasus Revolut terkait dengan sanksi, mengklaim bahwa sistem mereka dapat mendeteksi dan secara otomatis menghentikan transaksi kepada individu yang cocok dengan daftar sanksi. Namun, sistem tersebut hanya menandai transaksi untuk investigasi lebih lanjut dan tetap membiarkan transaksi tersebut berjalan. Akibatnya, sistem Revolut gagal mendeteksi penipuan massal, memungkinkan pencuri mencuri USD 20 juta dari kas perusahaan.

Teknologi Regulasi (*RegTech*) dan Relevansinya Dengan Berbagi Data Lintas Lembaga

Dari kasus pencucian uang dan penipuan yang dijelaskan di atas, jelas bahwa kekurangan sistem dapat menjadi celah yang menghambat lembaga keuangan dan berkontribusi pada risiko finansial dan reputasi mereka. Terutama jika implementasi sistem tidak sesuai dengan standar yang ditetapkan oleh regulator. Proses kepatuhan yang dapat diotomatisasi oleh Teknologi Regulasi (*RegTech*) meliputi uji tuntas pelanggan, pemantauan transaksi, dan pelaporan. Hal ini dapat membantu lembaga keuangan mematuhi regulasi secara lebih efisien dan efektif serta mengurangi risiko kesalahan dan tindakan hukuman. Menurut *Institute of International Finance* (IIF), *RegTech* dapat mencakup alat audit, pelaporan, kepatuhan (seperti penerapan KYC dan AML/CTF), dan manajemen risiko. Ini dapat dicapai dengan menghubungkan algoritma canggih dan model bisnis, kecerdasan buatan, pembelajaran mesin, dan pengawasan waktu nyata. Mengingat sifat era keuangan digital saat ini yang sangat bergantung pada data dan ditandai dengan velositas tinggi, variasi besar, dan volume besar data (disebut sebagai 3V), aspek-aspek ini sangat mungkin untuk beroperasi dan berkembang.¹⁵

¹⁵ Henrik Braun, "Evaluation of Big Data Maturity Models: A Benchmarking Study to Support Big Data Maturity Assessment in Organizations," 2015, 129, <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj1t4LKpN2EAxU8KbkGHQ3SCOCQFnoECA4QAQ&url=https%3A%2F%2Fcore.ac.uk%2Fdownload%2Fpdf%2F196555414.pdf&usg=AOvVaw3ng3KVN2-0l5wiXhkHFZ91&opi=89978449>.

RegTech pada dasarnya menggabungkan regulasi dan teknologi. Solusi *RegTech* mendorong digitalisasi dan inovasi digital, memengaruhi berbagai organisasi, entitas, dan otoritas, memberikan cara untuk memperbaiki area seperti pelaporan digital, yang berpotensi mengubah struktur yang ada dan membentuk kembali proses dan sistem regulasi.^{16, 17} Pendekatan berbasis data akan memperkenalkan paradigma baru atau menggeser paradigma yang ada. Misalnya, dari pendekatan KYC (*Know Your Customer*) ke KYD (*Know Your Data*).¹⁸ Ekosistem data muncul sebagai aspek kunci¹⁹ di mana data dibagikan "antarregulator, asosiasi industri, dan investor, yang merupakan dasar untuk regulasi berbasis teknologi yang terintegrasi".²⁰ Data dapat berupa terstruktur (seperti pesanan perdagangan dan pesanan yang dibatalkan, data pasar, dan portofolio pelanggan) atau tidak terstruktur (seperti email, rekaman suara, profil media sosial, atau komunikasi lainnya), kualitatif atau kuantitatif, dan terperinci atau teragregasi.²¹

Berbagi data lintas lembaga dengan infrastruktur yang baik dan akses yang aman sangat penting untuk mengoptimalkan implementasi *RegTech* di antara FI, regulator, asosiasi industri, dan investor. Saat ini, berbagi data di antara lembaga keuangan telah terjadi untuk sistem pembayaran, dan implementasi QRIS adalah salah satu contoh *open banking*. Hal ini konsisten dengan BSPI, yang menunjukkan peran bank sentral dalam mendukung interoperabilitas, persaingan, dan inovasi, serta pengoperasian infrastruktur publik. Inisiatif *open banking* melalui standarisasi antarmuka pemrograman aplikasi (*Application Programming Interfaces* - API) dan antarmuka pembayaran terintegrasi (*Integrated Payment Interfaces* - IPI) terbuka bertujuan untuk mendorong transformasi digital dalam perbankan dan mempromosikan keterhubungan antara *FinTech* dan bank.

Gagasan berbagi data lintas lembaga dalam pemantauan transaksi untuk menegakkan AML dapat mencerminkan bagaimana Bank Indonesia menstandarisasi API dan IPI sehingga pertukaran data antara lembaga keuangan dan regulator dapat diamankan dengan baik. Keuntungan yang dapat diperoleh lembaga keuangan dan regulator dari menerapkan *open banking* untuk pemantauan transaksi dalam AML adalah aktivitas penipuan dapat dikelola dengan baik melalui akses antar lembaga keuangan, regulator, dan lembaga mana pun yang terhubung dengan aktivitas tersebut. Ini akan membuat pekerjaan penyelidik lebih efektif dan efisien dalam menyelidiki kasus-kasus pencucian uang.

¹⁶ Douglas W. Arner et al., "Sustainability, FinTech and Financial Inclusion," *European Business Organization Law Review* 21, no. 1 (2020): 7–35, <https://doi.org/10.1007/s40804-020-00183-y>.

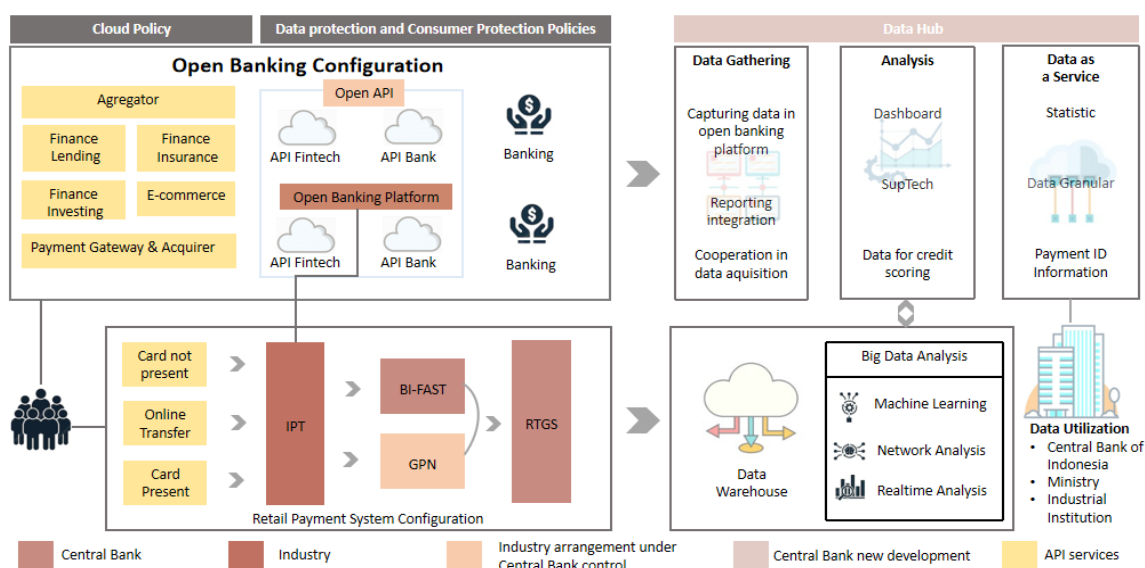
¹⁷ Petros Kavassalis et al., "The Journal of Risk Finance An Innovative RegTech Approach to Financial Risk Monitoring and Supervisory Reporting Article Information," *The Journal of Risk Finance* 19, no. 1 (2018): 1–18, <https://doi.org/10.1108/JRF-07-2017-0111>.

¹⁸ Arner, Barberis, and Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation."

¹⁹ Seán O’Riain, Edward Curry, and Andreas Harth, "XBRL and Open Data for Global Financial Ecosystems: A Linked Data Approach," *International Journal of Accounting Information Systems* 13, no. 2 (2012): 141–62, <https://doi.org/10.1016/j.accinf.2012.02.002>.

²⁰ Yang and Li, "Evolutionary Approaches and the Construction of Technology-Driven Regulations."

²¹ EIOPA, "Digital Transformation Strategy,"; Yang and Li, "Evolutionary Approaches and the Construction of Technology-Driven Regulations." 2021.

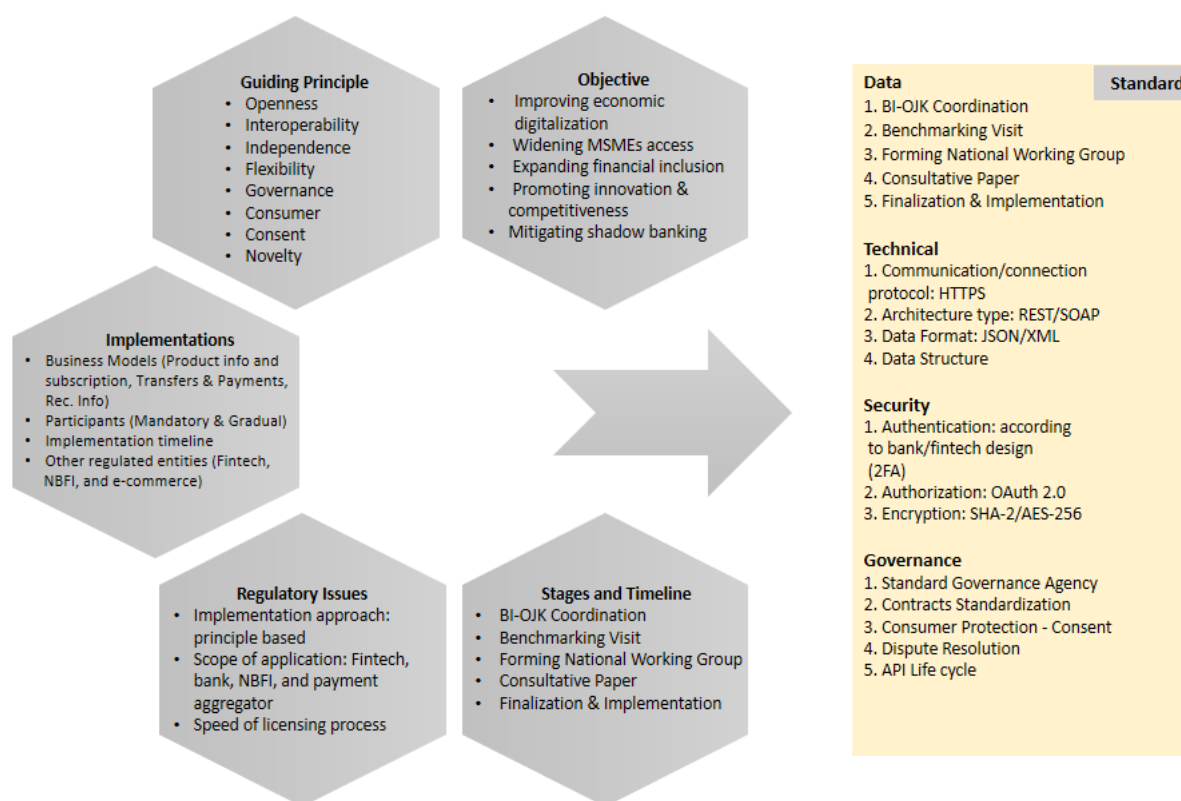


Gambar 1. Konfigurasi Open API SNAP Data-Hub

Sumber: Bank Indonesia, 2021

Standar Pembayaran Open API (SNAP) adalah seperangkat protokol dan instruksi yang memfasilitasi interkoneksi antar aplikasi dalam memproses transaksi pembayaran yang ditetapkan oleh Bank Indonesia. SNAP QRIS sendiri merupakan perwujudan dari Sistem Pembayaran Indonesia (SPI) 2025 selain *platform* yang sudah ada, yaitu Open API, BI-FAST, QRIS, IPT, BI-RTGS, Data Hub, Payment ID, Sandbox 2.0, dan sistem elektronik sebagai penggerak untuk tiga sektor, yaitu sektor ekonomi, sektor keuangan, dan Bank Indonesia sendiri.

SNAP, di sisi lain, sebagai Open API menempatkan dirinya sebagai sistem perantara yang menjadi jembatan komunikasi data antara *front-end* dan *back-end* yang berperan sebagai penggerak atau *data hub* untuk melakukan transaksi antara sistem jaringan bank sentral di berbagai negara ASEAN+ untuk melaksanakan penyelesaian transaksi.



Gambar 2. Kerangka Kebijakan Standar Open API

Sumber: Bank Indonesia, 2021

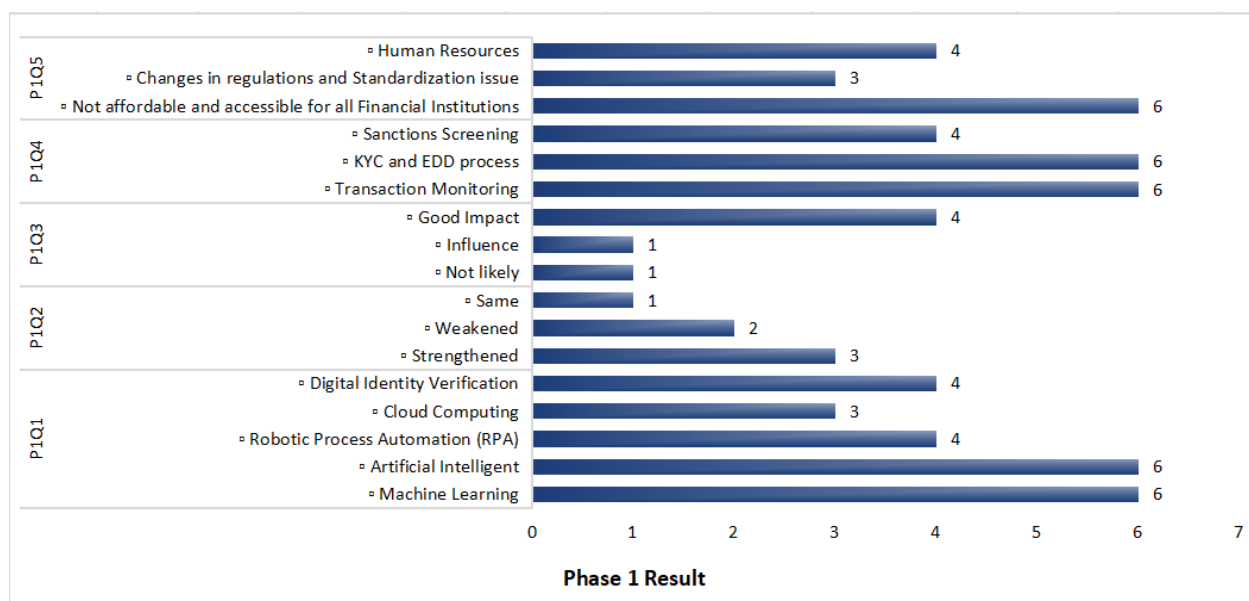
Dalam mengimplementasikan SNAP sebagai Open API, diperlukan dasar kerangka kerja yang harus dipatuhi sebagai standar tata kelola untuk menjadi Open API yang andal, berkelanjutan untuk pengembangan di masa depan, dan aman digunakan. Implementasi *open banking* bertujuan untuk mendukung transformasi digital dalam perbankan agar menjadi lebih lancar dan terintegrasi. Akibatnya, ini menjadi katalisator bagi perbankan dalam menstandarisasi Open API terkait standar data, pedoman teknis, tingkat, dan standar keamanan, serta tata kelola yang baik, sehingga bank tetap eksis dalam memberikan layanan bersama dengan berbagai layanan keuangan/*startup FinTech*.

Open Banking untuk Mengoptimalkan Pemantauan Transaksi AML

Menggunakan sistem atau pemahaman AML yang kuno dapat menyebabkan lembaga keuangan mengalami kerugian. Sebenarnya, hal ini dapat dihindari melalui analisis berbasis AI dan *big data*. Karena itu, bank dan lembaga keuangan lainnya harus mengadopsi metode kontemporer yang memungkinkan mereka tetap berada di depan dalam proses keuangan sambil memastikan kepatuhan regulasi yang menjamin efektivitas biaya dan efisiensi. Peningkatan pelanggaran keuangan dan kebutuhan akan protokol keamanan siber yang diperkuat telah menekankan pentingnya *RegTech*. Solusi *RegTech* dalam sektor kejahatan keuangan memanfaatkan teknik analisis *big data* yang canggih untuk meneliti sejumlah besar data dan menjalin hubungan antara titik data yang tampaknya tidak terkait, sehingga memperoleh perspektif regulasi yang komprehensif. Data ini dapat diakses melalui *open banking*, yang membangun koneksi langsung ke bank untuk pelacakan transaksi secara *real-time* yang lancar dan evaluasi risiko klien.

Menurut hasil survei Delphi yang dilakukan dan dikirimkan kepada para ahli dalam bidang AML dan *RegTech*, terdapat beberapa solusi *RegTech* memungkinkan untuk diterapkan. Keenam responden (100%) berhasil mengirimkan jawaban mereka untuk survei Fase 1. Hal ini dapat

diterima, mengingat penelitian ini memerlukan setidaknya lima spesialis AML atau *RegTech*. Survei ini terdiri dari lima pertanyaan terbuka yang menghasilkan jawaban teks bebas. Gambar 3 merangkum hasil yang diperoleh melalui analisis teks manual untuk setiap pertanyaan di Fase 1.



Gambar 3. Hasil Fase 1

Sama seperti Fase 1, Fase 2 memiliki tingkat respons sebesar 100% karena semua responden mengirimkan jawaban tepat waktu. Survei ini terdiri dari pertanyaan skala Likert yang berkisar dari 1 (tidak penting sama sekali) hingga 5 (sangat penting) dan dua pertanyaan tertutup untuk panel ahli untuk me-ranking jawaban mereka dari Fase 1. Survei untuk fase ini dibagi menjadi empat bagian, yaitu:

1. Kemajuan teknologi untuk kepatuhan AML;
2. Pencucian uang, *RegTech*, dan lembaga pengatur;
3. *RegTech* versus Kejahatan Keuangan; dan
4. Keterbatasan dan hambatan mendatang *RegTech* untuk kepatuhan AML.

Tujuan dari P2Q1 adalah untuk mengetahui perspektif responden mengenai masa depan solusi *RegTech* terkait kepatuhan AML (Tabel 1). Pertanyaan P2Q2 bertujuan untuk menilai dampak potensial dari penerapan teknologi canggih oleh lembaga keuangan dalam upaya anti-pencucian uang (AML) mereka terhadap tingkat kompleksitas teknik pencucian uang ilegal yang diadopsi oleh pelaku, sebagaimana digambarkan dalam Tabel 2. Tujuan P2Q3 adalah untuk memastikan apakah solusi *RegTech* memiliki potensi untuk melampaui saran regulator dalam ranah program dan pengembangan kebijakan AML di lembaga keuangan (seperti yang ditunjukkan oleh Tabel 3). P2Q4 bertujuan untuk menentukan topik selanjutnya yang akan ditangani oleh solusi *RegTech* terkait kepatuhan AML menurut para ahli (Tabel 4). P2Q4 bertujuan untuk memastikan hierarki prioritas para ahli mengenai tantangan masa depan dalam implementasi *RegTech* untuk kepatuhan AML, seperti yang disajikan dalam Tabel 5.

Tabel 1. Jawaban yang Disintesis dari Para Ahli untuk Pertanyaan 1 pada Tahap 2 (P2Q1)

P2Q1: Di bawah ini adalah kompilasi teknologi yang diidentifikasi oleh responden pada Fase 1 sebagai teknologi yang memiliki potensi terbesar untuk secara signifikan memengaruhi program kepatuhan AML dalam dekade berikutnya. Silakan beri penilaian Anda tentang signifikansi setiap teknologi terhadap kepatuhan AML dalam sepuluh tahun ke depan, dengan menggunakan sistem penilaian dari 1 ("Tidak penting sama sekali") hingga 5 ("Sangat penting").

Jawaban dari para ahli teknologi	Tidak penting sama sekali [1] dalam %	Tidak penting [2] dalam %	Netral [3] dalam %	Penting [4] dalam %	Sangat penting [5] dalam %
Machine Learning (P2Q1.1)	-	-	-	50%	50%
Artificial Intelligence (P2Q1.2)	-	16,7%	-	33,3%	50%
Robotic Process Automation (RPA) (P2Q1.3)	16,7%	-	50%	-	33,3%
Digital Identity Verification (P2Q1.4)	-	-	-	50%	50%
Cloud Computing (P2Q1.5)	-	-	16,7%	33,3%	50%

Konsensus dicapai untuk setiap pertanyaan pada Fase 2, kecuali untuk pertanyaan pertama (P2Q1) tentang otomatisasi proses robotik, yang dianggap kurang mungkin memiliki dampak signifikan pada program kepatuhan AML karena persentasenya kurang dari 50%. Konsensus terkuat di antara peserta untuk setiap topik yang dibahas pada akhir Fase 2 dijelaskan sebagai berikut:

- a. Pembelajaran Mesin (*Machine Learning*) dan verifikasi identitas digital (*Digital Identity Verification*) dinilai sebagai teknologi paling berdampak dalam program kepatuhan AML (100%), diikuti oleh kecerdasan buatan (*Artificial Intelligence*) dan komputasi awan (*Cloud Computing*) (83,3%). Teknologi ini mengubah cara layanan keuangan digital dalam mengidentifikasi pelanggan menggunakan verifikasi identitas digital dan mengotomatisasi tugas harian manual menggunakan pembelajaran mesin.

Tabel 2. Fase 2 - Jawaban yang Disintesis dari Para Ahli untuk Pertanyaan 2 (P2Q2)

P2Q2: Sejauh mana Anda percaya bahwa penerapan sistem teknologi canggih oleh lembaga keuangan untuk prosedur kepatuhan anti pencucian uang (AML) mereka akan memengaruhi kompleksitas taktik pencucian uang yang digunakan oleh penjahat? (Pilih salah satu)

Pilihan Jawaban	Jawaban Para Ahli dalam %
Metode Pencucian Uang akan menjadi lebih canggih	100%
Metode Pencucian Uang akan menjadi kurang canggih	-
Metode Pencucian Uang akan tetap sama	-

- b. Semua responden (100%) setuju bahwa penerapan teknologi canggih dalam program kepatuhan AML akan secara tidak terelakkan mendorong peningkatan kecanggihan teknik pencucian uang. Hal ini merupakan peringatan bagi layanan keuangan digital untuk meningkatkan kemampuan sistem AML agar tetap relevan dengan perkembangan teknologi. Selain itu, dengan memanfaatkan teknologi, sistem dapat mendeteksi dan menganalisis perilaku anomali potensial yang terkait dengan pencucian uang.

Tabel 3. Fase 2 - Jawaban yang Disintesis dari Para Ahli untuk Pertanyaan 3 (P2Q3)

P2Q3: Di masa depan, mungkinkah solusi *RegTech* akan memiliki dampak yang lebih besar daripada badan regulasi dalam merumuskan kebijakan anti pencucian uang (AML) di lembaga keuangan? (Pilih salah satu)

Pilihan Jawaban	Jawaban Para Ahli dalam %
Ya	83,3%
Tidak	16,7%

- c. Solusi *RegTech* telah dikonfirmasi memiliki pengaruh yang lebih besar daripada regulator dalam bagaimana kebijakan AML dirancang dalam lembaga keuangan (83,3%). Namun, regulator memiliki otoritas untuk mengatur dan mengarahkan kebijakan AML. Kegagalan untuk melakukan hal tersebut dapat mengakibatkan *RegTech* mengambil alih peran ini, yang jika digunakan secara tidak tepat, dapat berdampak negatif pada pengambilan keputusan yang tidak bias.

Tabel 4. Fase 2: Jawaban yang Disintesis dari Para Ahli untuk Pertanyaan 4 (P2Q4)

P2Q4: Di bawah ini adalah kompilasi topik yang telah diidentifikasi sebagai titik fokus potensial dalam kejahatan keuangan oleh responden dari Fase 1. Solusi *RegTech* dapat membantu dalam menangani kekhawatiran ini. Harap tunjukkan tingkat kesepakatan Anda dengan pentingnya penerapan solusi *RegTech* untuk setiap topik menggunakan skala penilaian dari 1 ("Tidak penting sama sekali") hingga 5 ("Sangat penting")

Jawaban dari para ahli teknologi	Tidak penting sama sekali [1] dalam %	Tidak penting [2] dalam %	Netral [3] dalam %	Penting [4] dalam %	Sangat penting [5] dalam %
Mengawasi Transaksi (P2Q4.1)	-	-	16,7%	-	83,3%
Proses KYC dan EDD (P2Q4.2)	-	-	-	33,3%	66,7%
Penyaringan Sanksi (P2Q4.3)	-	-	-	-	100%

- d. Penyaringan sanksi (100%) tercatat sebagai fokus berikutnya yang paling mungkin dalam kejahatan keuangan yang dapat dibantu oleh solusi *RegTech*. Selain itu, pemantauan transaksi dan proses *Know Your Customer* (KYC) dan *Enhanced Due Diligence* (EDD) juga memiliki potensi yang akan ditangani oleh solusi *RegTech* di masa depan, dengan persentase mencapai 83,3% dan 66,7% secara berurutan. Penyaringan sanksi telah mendapatkan perhatian signifikan di sektor ini, mengingat sifat layanan keuangan digital yang menawarkan layanan valuta asing. Hal ini untuk memastikan bahwa reputasi mereka tetap terjaga dan mereka tidak berhubungan dengan pihak yang dikenai sanksi atau masuk daftar hitam.

Tabel 5. Fase 2: Jawaban yang Disintesis dari Para Ahli untuk Pertanyaan 5 (P2Q5)

P2Q5: Di bawah ini adalah kompilasi kendala yang disebutkan oleh responden pada Fase 1 sebagai hambatan utama untuk menerapkan solusi *RegTech* di lembaga keuangan untuk kepatuhan AML. Harap nilai pentingnya setiap kendala menggunakan skala penilaian dari 1 ("Tidak penting sama sekali") hingga 5 ("Sangat penting")

Jawaban dari para ahli teknologi	Tidak penting sama sekali [1] dalam %	Tidak penting [2] dalam %	Netral [3] dalam %	Penting [4] dalam %	Sangat penting [5] dalam %
Tidak terjangkau dan susah diakses oleh semua Lembaga Keuangan (P2Q5.1)	-	-	16,7%	50%	33,3%
Perubahan regulasi dan masalah Standarisasi (P2Q5.2)	-	16,7%	16,7%	50%	16,7%
Sumber Daya Manusia (P2Q5.3)	-	16,7%	33,3%	16,7%	33,3%

- e. Implementasi solusi *RegTech* memiliki tantangan spesifik yang dikonfirmasi oleh responden sebagai tidak terjangkau dan tidak dapat diakses oleh semua institusi keuangan (83,3%), diikuti oleh perubahan dalam regulasi serta masalah standarisasi (66,7%) dan sumber daya manusia (50%). Ukuran layanan keuangan digital yang bervariasi telah menghasilkan kapasitas yang berbeda dalam menawarkan solusi *RegTech* yang komprehensif, karena perbedaan modal dan kelayakan anggaran yang melekat. Namun, hal ini tidak boleh menjadi hambatan signifikan, asalkan regulator memberikan panduan dan kebijakan khusus untuk memastikan kepatuhan di antara layanan keuangan digital.

Tabel 6. Rata-Rata Tanggapan Kelompok untuk Pertanyaan P2Q1, P2Q4, dan P2Q5

Pertanyaan	Opsi Respon	Rata-Rata Tanggapan Kelompok (1-5)	Mean absolute deviation (MAD)
P2Q1	<i>Machine Learning</i> (P2Q1.1)	4,5	0,5
	<i>Artificial Intelligence</i> (P2Q1.2)	4,2	0,8
	<i>Robotic Process Automation (RPA)</i> (P2Q1.3)	3,8	0,9
	<i>Digital Identity Verification</i> (P2Q1.4)	4,8	0,3
	<i>Cloud Computing</i> (P2Q1.5)	4,3	0,7
P2Q4	Mengawasi Transaksi (P2Q4.1)	4,7	0,6
	Proses KYC dan EDD (P2Q4.2)	4,7	0,4
	Penyaringan Sanksi (P2Q4.3)	5	0
P2Q5	Tidak terjangkau dan susah diakses oleh semua Lembaga Keuangan (P2Q5.1)	4,2	0,6
	Perubahan regulasi dan masalah Standarisasi (P2Q5.2)	3,7	0,8
	Sumber Daya Manusia (P2Q5.3)	3,7	1

Dalam survei Fase 1, analisis teks menegaskan bahwa teknologi canggih seperti pembelajaran mesin (*machine learning*), kecerdasan buatan (AI), otomatisasi proses robotik (RPA), komputasi awan (*cloud computing*), dan verifikasi identitas digital (*digital identity verification*) akan berdampak signifikan pada kepatuhan AML dalam lembaga keuangan. Berdasarkan pendapat para ahli yang disurvei, teknologi-teknologi ini telah disajikan sebagai opsi tanggapan untuk Fase 2 guna memprioritaskan dan menilai pemikiran mereka. Pada bagian ini, analisis data lebih difokuskan pada Fase 2 karena analisis tanggapan dari Fase 1 menjadi dasar desain survei untuk Fase 2.

Metode Delphi mengandalkan potensi para ahli yang disurvei untuk mencapai konsensus tentang topik tertentu melalui tanggapan anonim terhadap survei berturut-turut. Untuk memastikan analisis data yang akurat dan hasil mentah, perlu ditetapkan definisi konsensus untuk studi ini. Konsensus dianggap tercapai untuk nilai kategori (misalnya, pertanyaan Ya-Tidak) ketika lebih dari 50% peserta memberikan tanggapan yang sama. Untuk skala dan rasio (seperti skala Likert yang berkisar dari 1 hingga 5), konsensus dianggap tercapai ketika rata-rata tanggapan kelompok berada dalam interval [1;2] atau [4;5].

Analisis data Fase 2 difokuskan pada nilai kategori untuk pertanyaan Ya-Tidak dan pertanyaan tertutup (P2Q2, P2Q3) (Tabel 3, 4) serta perhitungan rata-rata tanggapan kelompok untuk skala dan rasio (P2Q1, P2Q4, P2Q5). Kategorisasi tersedia untuk pertanyaan 2 (P2Q2) untuk melanjutkan analisis data. Mengenai pertanyaan 2 dan 3 pada Fase 2 (P2Q2, P2Q3), konsensus tercapai pada kedua kasus tersebut, dengan tingkat persetujuan masing-masing 100% dan 83,3%. Ini berarti bahwa penggunaan solusi *RegTech* yang semakin meningkat oleh lembaga keuangan

untuk kepatuhan AML akan menyebabkan metode pencucian uang yang lebih canggih secara teknologi, dan solusi *RegTech* akan memiliki pengaruh yang lebih besar daripada rekomendasi regulator dalam merancang kebijakan AML di dalam lembaga keuangan.

Mean Absolute Deviation (MAD) adalah ukuran kuantitatif yang mengukur derajat variasi dalam satu set data relatif terhadap rata-ratanya. Perhitungan ini melibatkan rata-rata perbedaan absolut antara setiap nilai dan rata-ratanya. MAD yang lebih kecil menunjukkan bahwa titik data berkumpul erat di sekitar kecenderungan sentral, sedangkan MAD yang tinggi menunjukkan penyebaran atau dispersi yang lebih besar. MAD yang lebih rendah mengimplikasikan kedekatan dengan rata-rata dan variabilitas yang berkurang, yang dapat menunjukkan keandalan, konsistensi, atau keseragaman. Sebaliknya, MAD yang lebih tinggi menunjukkan penyimpangan signifikan dari rata-rata dan variabilitas yang meningkat yang dapat menunjukkan gangguan, ketidakstabilan, atau heterogenitas.

Menurut rata-rata tanggapan kelompok dalam Tabel 7 untuk pertanyaan P2Q1, P2Q4, dan P2Q5, lembaga keuangan disarankan untuk mempertimbangkan investasi dalam solusi *RegTech* sebagai sarana untuk memperkuat program kepatuhan anti-pencucian uang mereka dengan menggunakan verifikasi identitas digital untuk penyaringan sanksi, serta pembelajaran mesin dan kecerdasan buatan untuk pemantauan transaksi, proses KYC, dan EDD. Selain itu, lembaga keuangan harus memprioritaskan investasi dalam solusi *RegTech* untuk memperkuat kapasitas mereka dalam beradaptasi dengan teknologi yang muncul dan mempercepat kematangan program kepatuhan AML. Semakin cepat lembaga keuangan meningkatkan teknologi kepatuhan AML, semakin mempercepat implementasi *open banking* dalam hal kesiapan infrastruktur teknologi.

Kesimpulan

Mengimplementasikan sistem yang usang, seperti solusi AML kuno, dapat menyebabkan lembaga keuangan mengalami kerugian yang sebenarnya bisa dicegah dengan menggunakan analisis berbasis AI dan *big data*. Oleh karena itu, bank dan lembaga keuangan lainnya harus mengadopsi pendekatan modern yang memungkinkan mereka untuk tetap unggul dalam operasional keuangan sambil memastikan kepatuhan terhadap regulasi guna menjamin efektivitas biaya dan efisiensi.

Analisis data menunjukkan bahwa penggunaan teknologi canggih seperti pembelajaran mesin (*machine learning*) dan verifikasi identitas digital sebagai bagian dari solusi *RegTech* mempercepat efisiensi pemantauan transaksi serta proses KYC dan EDD dalam AML. Hal ini juga mendukung strategi dan rencana regulator dalam memerangi pencucian uang terkait dengan bagaimana kebijakan AML dirancang dalam lembaga keuangan. Selain itu, para responden menyarankan peningkatan pemantauan transaksi, penyaringan sanksi, serta proses KYC dan EDD sebagai isu berikutnya yang bisa ditangani oleh solusi *RegTech*.

Telah terbukti bahwa waktu akan menjadi sumber daya yang semakin krusial bagi lembaga keuangan untuk mengintegrasikan solusi *RegTech* agar tetap terdepan terkait perubahan regulasi *open banking* dan menghadapi perkembangan mendatang. Karena lembaga keuangan menghadapi penipu dan pelaku pencucian uang yang sama, bekerja sama dengan didukung oleh berbagi data lintas lembaga yang diaktifkan oleh sistem *open banking* akan meningkatkan lingkungan lembaga keuangan dalam hal menyediakan keamanan dan kestabilan bagi bank serta integritas sistem keuangan internasional. Regulator harus tetap sadar bahwa penjahat menggunakan metode pencucian uang yang semakin canggih. Oleh karena itu, regulator harus memantau *RegTech* dan sepenuhnya mengadopsi teknologi untuk meningkatkan kemampuan pengawasan mereka. Ini memerlukan perekrutan spesialis teknis tambahan yang dapat membantu dalam integrasi *RegTech* ke dalam kerangka regulasi.

Ucapan Terima Kasih

Atas nama Allo Bank, penulis ingin mengucapkan terima kasih kepada semua pihak yang telah memungkinkan studi ini dan atas dukungan terus-menerus mereka terhadap Allobank dalam upaya penelitiannya. Selain itu, kami ingin mengucapkan terima kasih kepada individu-individu berikut: Rika Astari (*RegTech.ID*), Pandu Adiat (Allo Bank), Muhammad Iqbal Saksono (ALAMI, mantan Kepala AML CFT - SeaBank), Christian PYK (Bank Sinarmas, mantan Pimpinan AML CFT - SeaBank), Kemal M (SeaBank), dan Robby Julian (SeaBank) atas kontribusi mereka dan kesediaan mereka untuk berpartisipasi sebagai responden sehingga studi ini dapat terlaksana.

Secara khusus, kami berterima kasih kepada Indra Utoyo (Direktur Utama Allo Bank), Dimas Hananto Nugroho (Kepala Kepatuhan & AML/CTF Allo Bank), dan Dewi Evarini (Kepala Departemen AML/CTF Allo Bank) atas usaha dan dukungan berharga mereka sepanjang studi ini.

Daftar Pustaka

- Arner, Douglas W., János Barberis, and Ross P. Buckley. "FinTech, RegTech, and the Reconceptualization of Financial Regulation." *Northwestern Journal of International Law and Business* 37, no. 3 (2017): 373–415.
- Arner, Douglas W., Ross P. Buckley, Dirk A. Zetzsche, and Robin Veidt. "Sustainability, FinTech and Financial Inclusion." *European Business Organization Law Review* 21, no. 1 (2020): 7–35. <https://doi.org/10.1007/s40804-020-00183-y>.
- Bank Indonesia. *Indonesia Payment Systems Blueprint 2025 Bank Indonesia: Navigating the National Payment Systems in the Digital Era* BA, 2019.
- Braun, Henrik. "Evaluation of Big Data Maturity Models: A Benchmarking Study to Support Big Data Maturity Assessment in Organizations," 2015, 129. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj1t4LKpN2EAXU8KbkGHQ3SCOcQFnoECA4QAQ&url=https%3A%2F%2Fcore.ac.uk%2Fdownload%2Fpdf%2F196555414.pdf&usg=AOvVaw3ng3KVN2-0l5wiXhkHFZ91&opi=89978449>.
- Butler, T. and Brooks, R. "On the Role of Ontology-Based RegTech for Managing Risk and Compliance Reporting in the Age of Regulation." *Journal of Risk Management in Financial Institutions* 11, no. 1 (2017): 19–33.
- Commission, European. "Report From The Commission To The European Parliament And The Council." *Angewandte Chemie International Edition*, 6(11), (2019): 951–952., <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0370&from=GA>.
- Demetis, Dionysios S. "Fighting Money Laundering with Technology: A Case Study of Bank X in the UK." *Decision Support Systems* 105 (2018): 96–107. <https://doi.org/10.1016/j.dss.2017.11.005>.
- EIOPA. "Digital Transformation Strategy," 2021.
- European Parliament. "Money Laundering - Recent Cases from a EU Banking Supervisory Perspective," no. February (2018): 1–24. https://www.europarl.europa.eu/cmsdata/142725/EGOV_Briefing_on_EU_Banking_supervisory_perspective.pdf.
- Kavassalis, Petros, Harald Stieber, Wolfgang Breymann, Keith Saxton, and Francis Gross. "The Journal of Risk Finance An Innovative RegTech Approach to Financial Risk Monitoring and Supervisory Reporting Article Information." *The Journal of Risk Finance* 19, no. 1 (2018): 1–18. <https://doi.org/10.1108/JRF-07-2017-0111>.
- Kurum, Esman. "RegTech Solutions and AML Compliance: What Future for Financial Crime?" *Journal of Financial Crime* 30, no. 3 (2023): 776–94. <https://doi.org/10.1108/JFC-04-2020-0051>.
- Lai, K. "Blockchain as AML Tool: A Work in Progress." *International Financial Law Review*,

- London, 2018.
- Lee, Emily. "Financial Inclusion: A Challenge to the New Paradigm of Financial Technology, Regulatory Technology and Anti-Money Laundering Law." *SSRN Electronic Journal*, (2018): 1–51. <https://doi.org/10.2139/ssrn.3018960>.
- O’Riain, Seán, Edward Curry, and Andreas Harth. "XBRL and Open Data for Global Financial Ecosystems: A Linked Data Approach." *International Journal of Accounting Information Systems* 13, no. 2 (2012): 141–62. <https://doi.org/10.1016/j.accinf.2012.02.002>.
- The, Dermot. "BIROn - Birkbeck Institutional Research Online The Politics of FinTech : Technology, Regulation and Disruption" 99 (2021): 859–72. <https://eprints.bbk.ac.uk/id/eprint/43244/10/43244a.pdf>.
- Yang, Dong, and Min Li. "Evolutionary Approaches and the Construction of Technology-Driven Regulations." *Emerging Markets Finance and Trade* 54, no. 14 (2018): 3256–71. <https://doi.org/10.1080/1540496X.2018.1496422>.
- Zetsche, Dirk A., Ross P. Buckley, Douglas W. Arner, and Janos Nathan Barberis. "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation." *SSRN Electronic Journal*, January (2017). <https://doi.org/10.2139/ssrn.3018534>.