

## Original paper

# AML Berbasis AI: Kepatuhan Cerdas atau Ancaman HAM Tersembunyi?

**Kartini Laras Makmur**

University of Warwick-UK

Korespondensi penulis: Kartini.Makmur@warwick.ac.uk

## Kata Kunci:

Hak Asasi Manusia, Kecerdasan  
Buatan,  
Pencucian Uang

## Abstrak

Kecerdasan buatan (AI) semakin banyak digunakan oleh bank untuk mendeteksi dan mencegah pencucian uang; namun, adopsi kerangka kerja anti pencucian uang (*anti-money laundering-AML*) berbasis AI menimbulkan kekhawatiran akan perlindungan hak asasi manusia (HAM). Makalah ini mengkaji cara-cara AI membantu AML di sektor perbankan, konsekuensi etika dan HAM dari implementasinya, dan sejauh mana strategi ini mematuhi uji proporsionalitas pada hukum HAM Indonesia. Berdasarkan analisis dokumen terstruktur dari peraturan dan literatur sekunder terkait, penelitian ini menemukan bahwa aplikasi AI harus menghormati privasi dan proporsional dalam mengatasi pelanggaran pencucian uang, sebagaimana ditegaskan oleh konstitusi dan peraturan Indonesia. Temuan ini menyoroti kebutuhan mendesak akan kerangka hukum yang komprehensif untuk memandu penggunaan AI dalam AML, menegakkan keadilan, akuntabilitas, dan transparansi dibarengi dengan menjaga HAM.

Dikirimkan: 13 November 2024

Diterima: 24 Juni 2025

Diterbitkan: 27 Juni 2025

Copyright (c) Author



**Untuk mensitasi artikel ini:** Makmur, K. L. 2025. *AML Berbasis AI: Kepatuhan Cerdas atau Ancaman HAM Tersembunyi?*. *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 3(2):249-270, <https://doi.org/10.59593/amlcft.2025.v3i2.251>

## Pendahuluan

Isu pencucian uang merupakan ancaman signifikan bagi lembaga keuangan dan masyarakat secara keseluruhan. Efek pencucian uang pada ekonomi sangat jelas, dikarenakan ini bisa mendorong pertumbuhan bisnis ilegal yang dapat mengacaukan ekonomi.<sup>1</sup> Kegiatan keuangan ilegal berpotensi merusak keseimbangan ekonomi dengan meningkatkan pengangguran dan inflasi, mengurangi potensi ekonomi, dan mengalihkan sumber daya yang diperlukan untuk mendanai kepentingan publik, seperti pendidikan dan layanan kesehatan, pertahanan dan keamanan nasional, infrastruktur, dan keadilan.<sup>2</sup>

<sup>1</sup> Ayodeji Aluko and Mahmood Bagheri, "The Impact of Money Laundering on Economic and Financial Stability and on Political Development in Developing Countries: The Case of Nigeria," *Journal of Money Laundering Control* 15, no. 4 (2012): 442–57, <https://doi.org/10.1108/13685201211266024>.

<sup>2</sup> Kartini Makmur and Ahsanul Minan, "Money Laundering/Financing of Terrorism Risks in the Indonesian Islamic Banking System," in *Proceedings of the 3rd International Conference of Islamic Finance and Business, ICIFEB 2022, 19-20 July 2022 (The 3rd International Conference of Islamic Finance and Business (ICIFEB 2022), Jakarta, Indonesia: EAI, 2023)*, 10–21, <https://doi.org/10.4108/eai.19-7-2022.2328202>.

Pencucian uang digunakan oleh individu yang terlibat dalam kegiatan melanggar hukum untuk menyembunyikan sumber keuntungan ilegal mereka. Alasan utama tindakan pencucian uang di Indonesia meliputi korupsi, kegiatan kriminal terorganisir, penipuan keuangan, transaksi narkoba terlarang, dan pendanaan untuk kegiatan teroris.<sup>3</sup> Pencucian uang mencakup berbagai kegiatan, termasuk pergerakan dana atau aset ilegal, akuisisi, transformasi, atau pemanfaatan keuntungan yang diperoleh secara tidak sah, dan pemberian saran, dukungan, dan bantuan dalam upaya pencucian uang.

Meskipun estimasi paling komprehensif yang tersedia saat ini hanya mencakup periode antara 1989 dan 2017, estimasi tersebut menunjukkan bahwa Indonesia mengalami arus masuk keuangan ilegal sekitar USD 101,49 miliar dan arus keluar sekitar USD 40,58 miliar dari enam komoditas ekspor teratasnya secara kumulatif.<sup>4</sup> Jumlah arus keluar modal ilegal tahunan tersebut mencapai 10% dari anggaran negara, sedangkan masuknya modal ilegal setara dengan 29%.<sup>5</sup> Data terbaru masih belum tersedia, menegaskan adanya tantangan dalam melacak arus keuangan ilegal dengan presisi

Lembaga keuangan tetap menjadi jalur utama dalam memfasilitasi upaya kriminal ini. Sekitar 50% organisasi keuangan menyatakan kesediaan untuk mendedikasikan sumber daya dalam mengoptimalkan teknologi sebagai elemen penting dari rencana investasi mereka untuk memerangi operasi pencucian uang.<sup>6</sup> Bank-bank di kawasan Asia Pasifik diperkirakan untuk meningkatkan tingkat investasi mereka terhadap *compliance technology* sepanjang tahun 2022.<sup>7</sup> Lexis Nexis menyatakan bahwa 49% bank melaporkan ekspektasi pertumbuhan anggaran, dengan tambahan 34% menyatakan ekspektasi mereka akan peningkatan yang signifikan.<sup>8</sup> Bank-bank di Indonesia, Australia, Thailand, dan Filipina telah mengindikasikan keinginannya untuk berinvestasi secara signifikan pada tahun 2023.<sup>9</sup>

AI diharapkan menjadi teknologi yang efektif untuk mengatasi masalah pencucian uang. Sejumlah bank telah menguji AI untuk analisis dalam meninjau kepatuhan dan meningkatkan kinerja AML selama beberapa periode. Terdapat lima metode yang membuat AI dapat meningkatkan sistem AML yang ada, yaitu otomatisasi pengumpulan data, redistribusi sumber daya melalui penilaian risiko klien dan prioritas peringatan, pemanfaatan analisis tautan, segmentasi, dan peningkatan deteksi anomali.<sup>10</sup> Perbaikan ini dapat dicapai dengan mengidentifikasi pola yang mencurigakan atau mengungkap pola baru.<sup>11</sup>

Namun, integrasi AI dalam AML menimbulkan kekhawatiran mengenai perlindungan hak asasi manusia (HAM), sehingga dibutuhkan perlindungan yang kuat. Masalah utama dalam konteks ini termasuk etika, tata kelola, akuntabilitas, dan privasi, yang semakin menonjol karena kemajuan pesat teknologi *machine learning*. Mengatasi tantangan yang kompleks dan saling terkait ini membutuhkan penyelarasan strategi AML berbasis AI dengan prinsip-prinsip HAM, khususnya di Indonesia, di mana beragam keyakinan budaya menambahkan dimensi pada tatanan etika dan peraturan.

---

<sup>3</sup> Kartini Laras Makmur, "Women and Dirty Money: How Women Are Affected by, Involved, and Counter Money Laundering," *Jurnal Hukum Prasada* 9, no. 1 (2022): 35–44, <https://doi.org/10.22225/jhp.9.1.2022.35-44>

<sup>4</sup> Widya Kartika et al., "Highlighting Illicit Financial Flow of Indonesia's Top Six Export Commodities," *Prakarsa Policy Brief* 17 (2019): 1–4

<sup>5</sup> Kartika et al.

<sup>6</sup> Digital Finance, "Asia Banks Spend \$45 Billion on Compliance – For What?," *Digital Finance*, March 13, 2024, <https://www.digfingroup.com/compliance-lexisnexis/>.

<sup>7</sup> Digital Finance.

<sup>8</sup> Digital Finance.

<sup>9</sup> Digital Finance.

<sup>10</sup> Howard Chitimira, Elfes Torerai, and Lisa Jana, "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector," *Potchefstroom Electronic Law Journal* 27 (2024): 1–30, <https://doi.org/10.17159/1727-3781/2024/v27i0a18024>

<sup>11</sup> Chitimira, Torerai, and Jana.

Makalah ini menawarkan kontribusi dengan membahas penggunaan AI di kerangka AML dalam kerangka hukum khusus Indonesia. Tidak seperti penelitian sebelumnya yang berfokus pada Eropa atau global dan didasarkan pada standar internasional seperti rekomendasi *Financial Action Task Force* (FATF), Peraturan Perlindungan Data Umum Uni Eropa (*European Union General Data Protection Regulation*), atau Konvensi Eropa tentang Hak Asasi Manusia (*European Convention on Human Rights*),<sup>12</sup> studi ini menerapkan uji proporsionalitas Indonesia berdasarkan Pasal 28J UUD 1945, bersama dengan undang-undang domestik seperti Undang-Undang Nomor 8 Tahun 2010 tentang AML dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi Elektronik dan Transaksi. Bertrand et al., juga menyoroti potensi AI dalam AML, seperti melalui otomatisasi *Customer Due Diligence* (CDD), *Know Your Customer* (KYC) dan pemantauan transaksi, serta mengkritik risiko HAM AI menggunakan standar hukum Uni Eropa.<sup>13</sup> Sebaliknya, makalah ini mengkaji bagaimana AI digunakan oleh bank-bank Indonesia dan mengevaluasi praktiknya terhadap prinsip etika dan konstitusional dalam konteks yang ditandai dengan rezim privasi yang berkembang dan kurangnya regulasi khusus tentang AI. Dengan menawarkan analisis yang didasarkan secara konstitusional lokal, studi ini mengisi kekosongan dalam literatur, terutama untuk Indonesia dan negara-negara Global Selatan lainnya yang menghadapi tantangan serupa. Karena Eropa beroperasi dalam lingkungan peraturan yang matang, namun Indonesia menggunakan undang-undang dan praktik industri yang terpecah-pecah, menggambarkan risiko global yang lebih luas bahwa AML berbasis AI dapat melanggar HAM tanpa pengawasan dan perlindungan hukum yang kuat.

Kebaruan makalah ini terletak pada kontribusinya yang tiga lapis. Pertama, makalah ini menawarkan integrasi AI, kerangka kerja AML, dan hukum HAM Indonesia dengan secara sistematis menerapkan uji proporsionalitas yang berakar pada yurisprudensi Eropa untuk Pasal 28J Konstitusi Indonesia, sehingga melokalkan alat hukum trans-nasional untuk menilai kepatuhan AI dalam konteks Indonesia. Kedua, makalah ini memberikan penilaian mendasar tentang penggunaan AI dalam praktik AML Indonesia, melampaui diskusi teoritis global untuk memetakan bagaimana teknologi seperti *machine learning* untuk pemantauan transaksi, sistem e-KYC, dan algoritme penilaian risiko yang berinteraksi dengan kewajiban hukum nasional, terutama yang diberlakukan oleh lembaga seperti Pusat Laporan dan Analisis Transaksi Keuangan Indonesia (PPATK), sambil menyoroti risiko hukum dan etikanya. Ketiga, makalah ini mengajukan proposal reformasi hukum baru untuk mengubah undang-undang AML Indonesia dengan memperkenalkan hak pemberitahuan pasca-pelaporan bagi individu yang ditandai oleh sistem AI, bergantung pada pembenaran penegakan hukum, sehingga mempromosikan keseimbangan antara transparansi dan integritas investigasi sejalan dengan konstitusi dan standar HAM internasional sebagai pendekatan yang belum dibahas dalam literatur AI-AML yang ada.

Makalah ini adalah studi hukum deskriptif-normatif yang meneliti penggunaan teknologi AI dalam sistem AML, berfokus pada integrasinya ke dalam fungsi kepatuhan perbankan seperti CDD, KYC, dan pemantauan transaksi. Makalah ini membahas manfaat operasional dan tantangan hukum-etis dari penerapan AI, termasuk kekhawatiran tentang privasi, bias algoritma, dan HAM. Uji proporsionalitas digunakan sebagai kerangka konstitusional sehingga makalah ini membahas pengamanan peraturan untuk memastikan bahwa strategi AML berbasis AI selaras dengan Konstitusi Indonesia 1945 dan standar HAM.

---

<sup>12</sup> See Martin Jullum et al., "Detecting Money Laundering Transactions with Machine Learning," *Journal of Money Laundering Control* 23, no. 1 (2020): 173–86, <https://doi.org/10.1108/jmlc-07-2019-0055>; Astrid Bertrand, Winston Maxwell, and Xavier Vamparys, "Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?," *SSRN Electronic Journal* (2020): 1–27, <https://doi.org/10.2139/ssrn.3647420>.

<sup>13</sup> Bertrand, Maxwell, and Vamparys, "Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?"

Makalah ini menggunakan metodologi *desk study* untuk menyelidiki kompatibilitas deteksi pencucian uang berbasis AI di industri perbankan Indonesia dengan prinsip-prinsip HAM. Metode analisis dokumen digunakan untuk memeriksa regulasi teknik anti pencucian uang berbasis AI. Studi ini berfokus pada pemahaman sumber undang-undang hukum dan memeriksa apa klausul batasannya secara menyeluruh dengan menggunakan uji proporsionalitas.

Makalah ini mengeksplorasi bagaimana uji proporsionalitas dapat digunakan untuk mengatasi masalah yang timbul dalam pencegahan pencucian uang berbasis AI di industri perbankan Indonesia sambil memastikan perlindungan HAM. Uji proporsionalitas memastikan bahwa kerangka kerja AML berbasis AI di Indonesia tidak melanggar HAM yang fundamental, seperti privasi dan proses hukum, dengan mengharuskan semua pembatasan yang ada bersifat sah, diperlukan, dan mengganggu secara minimal. Karena teknologi AI dalam AML berkembang lebih kuat dan menyebar, uji proporsionalitas memberikan kerangka hukum dan etika untuk menilai apakah penggunaannya memang dibenarkan dan seimbang.

Hasil penelitian ini dapat meningkatkan efektivitas upaya anti pencucian uang di industri perbankan Indonesia. Makalah ini menawarkan analisis konseptual dan hukum tentang bagaimana AI digunakan dalam praktik AML dan bagaimana teknologi ini bersinggungan dengan masalah HAM. Namun, tetap terdapat batasan penelitian, terutama tidak adanya data empiris tentang praktik penggunaan alat AML berbasis AI, bagaimana keputusan algoritmik dibuat, dan bagaimana individu yang ditandai terpengaruh. Studi ini juga tidak menggunakan perspektif dari pemegang hak dan pengalaman hidup mereka yang berpotensi menjadi sasaran pengawasan yang diskriminatif. Selain itu, meskipun makalah ini menyoroti kesenjangan peraturan yang ada di Indonesia, makalah ini tidak secara komprehensif menyelidiki dinamika kelembagaan dan politik yang membentuk tata kelola AI, juga tidak menawarkan komparasi bagaimana negara lain yang serupa mengatasi tantangan ini. Terakhir, meskipun uji proporsionalitas diperkenalkan sebagai standar hukum utama, makalah ini tidak mengeksplorasi bagaimana uji proporsionalitas ditegakkan atau ditafsirkan oleh pengadilan Indonesia.

## Pemanfaatan AI dalam AML

Pada tahun 1955, John McCarthy, profesor matematika dari *Dartmouth College*, memperkenalkan istilah "kecerdasan buatan", mempersiapkan panggung untuk bidang-bidang transformatif.<sup>14</sup> AI adalah bidang khusus dalam ilmu komputer yang berfokus pada pengembangan algoritma dan sistem yang memungkinkan mesin menunjukkan kemampuan kognitif seperti manusia.<sup>15</sup> Pengembangan mesin "cerdas" yang mampu menunjukkan pemikiran, komunikasi, dan perilaku seperti manusia telah terbukti efektif.

AI mencakup beberapa subbidang, salah satunya adalah *machine learning*. Mesin memiliki kemampuan untuk memperoleh pengetahuan dengan memproses dan mengasimilasi data secara mandiri. *Machine learning* memfasilitasi akuisisi kemampuan pengenalan pola dan kemampuan prediksi oleh suatu sistem secara otomatis.<sup>16</sup> Salah satu elemen penting dari *supervised machine learning* adalah intervensi manusia dalam penggunaan data berlabel, yang mencakup atribut seperti usia, pembayaran, waktu, dan Lokasi, untuk melatih model.<sup>17</sup> . Selanjutnya, *database* harus dikategorikan dengan tepat untuk mendapatkan efek yang

---

<sup>14</sup> Gil Press, "Artificial Intelligence (AI) Defined," *Forbes*, August 27, 2017, <https://www.forbes.com/sites/gilpress/2017/08/27/artificial-intelligence-ai-defined/>.

<sup>15</sup> Chitimira, Torerai, and Jana, "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector."

<sup>16</sup> Jullum et al., "Detecting Money Laundering Transactions with Machine Learning."

<sup>17</sup> Jullum et al.

diinginkan, seperti memfasilitasi proses persetujuan aplikasi kartu kredit.<sup>18</sup> Sebaliknya, *unsupervised learning* adalah teknik yang melibatkan konstruksi model *machine learning* tanpa pemanfaatan data berlabel atau campur tangan manusia dalam permodelannya.<sup>19</sup>

Berbagai lembaga keuangan telah menggunakan teknologi AI ke dalam sistem mereka untuk mengidentifikasi dan mencegah aktivitas kriminal, termasuk pencucian uang. Efisiensi sistem perbankan bergantung pada kebenaran informasi yang diberikan oleh konsumen, yang digunakan untuk mengawasi transaksi yang sah atau yang berpotensi ilegal. AI memeriksa klien dan transaksi untuk mengidentifikasi perilaku yang berpotensi mencurigakan. Pemeriksaan ditandai dengan otomatis, menggabungkan pendekatan khusus berdasarkan aturan yang telah ditentukan. Selanjutnya, operator manusia memeriksa hasil penandaan yang membutuhkan perhatian secara menyeluruh dan mengambil langkah-langkah yang diperlukan. Langkah-langkah tersebut bisa melibatkan intervensi manual seperti menyetujui, menolak, atau menghalangi transaksi. Proses manual menganalisis transaksi dapat menjadi tantangan yang signifikan bagi operator manusia, terutama bila sistem menghasilkan sejumlah besar data positif yang palsu.

### ***Customer Due Diligence Berbasis AI***

Sebagaimana disyaratkan oleh UU AML Indonesia, karyawan bank bertanggung jawab untuk memverifikasi keaslian dan kredibilitas dokumen yang diserahkan oleh klien selama proses pendaftaran. Agar mendapatkan pengetahuan yang komprehensif tentang individu yang terlibat dengan bank, bank menggunakan prosedur CDD. Prosedur CDD membantu mengidentifikasi dan menilai potensi risiko klien. Prosedur KYC juga digunakan untuk verifikasi keaslian klaim klien, dokumen resmi seperti kartu tanda penduduk (KTP), akta kelahiran, surat izin mengemudi (SIM), paspor, bukti alamat, atau kredensial relevan lainnya diperlukan oleh bank.<sup>20</sup>

CDD juga membantu bank dalam memahami sifat bisnis dan sumber pendapatan atau aset klien. Fitur ini memudahkan pemantauan dan deteksi perilaku yang berpotensi berbahaya, seperti menandai adanya perubahan jaringan transaksi, frekuensi, dan kuantitas. Menurut pedoman yang ditetapkan oleh FATF, bank disarankan untuk melakukan prosedur CDD ketika klien menjalin hubungan bisnis baru atau terlibat dalam transaksi di atas ambang batas yang telah ditentukan.<sup>21</sup> Memperbarui CDD ketika ada perubahan operasi memungkinkan bank untuk memperbarui dan memelihara profil klien mereka secara akurat dan memfasilitasi pemantauan berkelanjutan terhadap aktivitas yang berpotensi bermasalah.

FATF telah menguraikan karakteristik utama yang perlu dipantau dalam setiap transaksi, yaitu pergerakan dan tujuan klien, jenis pertukaran mata uang yang terlibat, serta batas transaksi, frekuensi, jumlah dan nilai.<sup>22</sup> Saat ini, banyak bank mengandalkan proses manual yang tidak terstandar untuk menilai risiko pelanggan. Metode yang memakan waktu dan sangat subjektif. Petugas kepatuhan mengumpulkan informasi tentang faktor-faktor seperti industri, yurisdiksi, dan produk, sayangnya seringkali menilai berdasarkan subjektifitas dan individual daripada berdasarkan kriteria yang standar. Pendekatan ini membebani petugas kepatuhan dan pelanggan, karena petugas sering ditugaskan untuk penyelidikan ekstensif pada dokumen yang diberikan, seperti laporan bank dan pengajuan pajak, tanpa kerangka kerja yang jelas. Metode subjektif ini menghasilkan penilaian risiko yang tidak konsisten dengan hasil yang sangat

---

<sup>18</sup> Jullum et al.

<sup>19</sup> Jullum et al.

<sup>20</sup> AML Law Number 8 Tahun 2010, Art. 19.

<sup>21</sup> FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," FATF-GAFI, last modified 2023, <https://www.fatf-gafi.org/content/dam/fatf-gafi/Recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>.

<sup>22</sup> FATF.

bervariasi di antara petugas kepatuhan, membuat prosesnya tidak dapat diandalkan dan tidak efisien.

Model *machine learning* menawarkan pendekatan alternatif berbasis data untuk CDD, meningkatkan kekuatan prediksi penilaian risiko. Tidak seperti kartu skor petugas, model ini mengandalkan data historis dan pola perilaku sehingga menghasilkan wawasan potensi kejahatan keuangan yang lebih akurat.<sup>23</sup> Model *machine learning* menjalani pengembangan dan pengujian untuk menyempurnakan akurasi prediktifnya sehingga memungkinkan lembaga keuangan mengidentifikasi pelanggan berisiko tinggi dengan lebih efektif. Dengan menggunakan *machine learning*, bank berpotensi mengotomatisasi sebagian proses CDD, meningkatkan efisiensinya, dan mengurangi beban kerja pada staf kepatuhan.

Uji tuntas yang berkelanjutan juga penting, karena bank mengumpulkan lebih banyak data perilaku pasca-orientasi. Informasi seperti volume transaksi, metode pembayaran, dan rekan bisnis menambahkan wawasan berharga untuk memperbarui peringkat risiko pelanggan secara dinamis. Model statistik dapat mengubah data transaksi ini menjadi skor risiko yang diperbarui dan membantu prediksi kemungkinan kejahatan keuangan. Pemantauan berkelanjutan ini juga dapat mengelompokkan pelanggan ke dalam kategori risiko berdasarkan pola perilaku, memungkinkan pemantauan pada segmen berisiko tinggi secara detail. Model-model ini membantu mengidentifikasi potensi pencucian uang, penghindaran pajak, atau pendanaan terorisme, meningkatkan kemampuan lembaga keuangan untuk merespons ancaman secara proaktif.

Mengintegrasikan hasil *machine learning* ke dalam sistem berbasis AI cerdas dapat mengoptimalkan proses CDD. Program AI menghasilkan laporan berkala yang mencakup peringkat risiko, lokasi transaksi, arah transaksi (masuk atau keluar), dan persentase transaksi yang bisa dikategorikan berdasarkan jenis.<sup>24</sup> Dengan mengotomatisasikan pengambilan keputusan, sistem AI ini dapat meningkatkan akurasi, kecepatan, dan efisiensi biaya dalam penilaian risiko pelanggan. Transformasi digital dan AI dapat menghemat sumber daya dan mengurangi biaya kepatuhan, menjadikan CDD suatu proses yang dapat diskalakan dan berkelanjutan. Seiring meningkatnya tekanan dalam bisnis dan peraturan, transisi ke solusi uji kepatuhan yang otomatis didukung AI tidak dapat dihindari lagi, agar lembaga keuangan bisa melakukan uji kepatuhan secara lebih efektif dan efisien di masa depan.

### ***Know Your Customer Berbasis AI***

Dalam konteks kepatuhan AML, KYC dan CDD adalah proses regulasi yang saling melengkapi namun berbeda dan harus diterapkan oleh lembaga keuangan. KYC melibatkan identifikasi awal dan verifikasi identitas pelanggan pada saat orientasi, menggunakan dokumen resmi seperti KTP, paspor, atau bukti alamat. Tujuannya adalah untuk mencegah akses anonim atau penipuan ke dalam sistem keuangan, memastikan bahwa hanya entitas yang dapat dilacak dan sah yang dapat bertransaksi. Di Indonesia, prosedur KYC diamanatkan oleh UU No. 8 Tahun 2010 dan semakin difasilitasi oleh sistem elektronik (e-KYC) yang terintegrasi dengan *database* pemerintah untuk memudahkan verifikasi identitas. Sebaliknya, CDD menggunakan pemeriksaan identitas untuk menilai profil risiko pelanggan melalui evaluasi berkelanjutan terhadap aktivitas keuangan, hubungan bisnis, dan potensi tautan ke entitas atau yurisdiksi yang berisiko tinggi. Ini memungkinkan bank untuk memantau perilaku dari waktu ke waktu dan menerapkan uji tuntas untuk klien berisiko tinggi. Perbedaan antara KYC dan CDD sangat penting untuk memahami bagaimana AI membentuk kembali kepatuhan sambil menimbulkan perhatian baru tentang pelanggaran HAM.

Undang-Undang No. 8 Tahun 2010 tentang Penanggulangan dan Pemberantasan Pencucian Uang dan serangkaian undang-undang nasional mewajibkan bank untuk melakukan

---

<sup>23</sup> Jullum et al., "Detecting Money Laundering Transactions with Machine Learning."

<sup>24</sup> Jullum et al.

beberapa hal, seperti prosedur KYC, mengidentifikasi orang yang terpapar politik, mengidentifikasi transaksi di negara berisiko tinggi, dan melaporkan transaksi yang mencurigakan atau tidak biasa.<sup>25</sup> Bank wajib mengidentifikasi transaksi yang berpotensi mencurigakan secara proaktif dan segera memberi tahu PPATK, yang berfungsi sebagai unit intelijen keuangan (*financial intelligence unit*-FIU) yang ditunjuk.<sup>26</sup> Kewajiban pelaporan tersebut tidak memerlukan pengungkapan kegiatan ini kepada pelanggan yang terlibat. Undang-undang kepatuhan, seperti undang-undang antikorupsi, memerlukan penerapan mekanisme seperti *whistleblowing* untuk mengidentifikasi dan mengungkap perilaku terlarang dalam entitas perusahaan. Sebaliknya, undang-undang AML mengamanatkan bank untuk mengambil peran sebagai informan pemerintah, yang sebenarnya dapat berpotensi bertentangan dengan kewajiban adat mereka untuk menjaga kerahasiaan pelanggan.

Namun, entitas keuangan seperti bank, pihak pemroses pembayaran, lembaga kredit, dan perusahaan asuransi memiliki kewajiban ini karena alasan yang kritis. Pertama, kecanggihan teknik pencucian uang menuntut pengawasan ketat dan hanya lembaga keuangan yang memiliki informasi yang diperlukan untuk mendeteksi transaksi yang mencurigakan dalam hubungan pelanggan.<sup>27</sup> Kedua, bank menghadapi insentif keuangan yang substansial untuk mengabaikan dana terlarang. Tanpa persyaratan hukum untuk mengidentifikasi dan melaporkan aktivitas yang mencurigakan, potensi keuntungan ekonomi dapat mendorong bank untuk menerima setoran uang yang melanggar hukum, kecuali dalam kasus kriminal yang terang-terangan.<sup>28</sup>

Lembaga keuangan mengumpulkan data dari calon klien untuk meningkatkan kualitas layanan mereka. Bank memanfaatkan data klien untuk menilai risiko yang terkait dengan pinjaman, mendeteksi kasus pencucian uang, dan mengidentifikasi potensi tindakan penipuan. Bank berkewajiban untuk berkolaborasi dengan pihak berwenang dalam kasus yang melibatkan pencucian uang dengan memberikan informasi terkait yang dapat berfungsi sebagai barang bukti dalam proses hukum. Akuisisi data yang berpusat pada pelanggan sangat penting dalam industri perbankan, mengingat perbankan *online* sudah terjadi dan meningkatnya prevalensi tindakan penipuan.

Teknologi AI digunakan oleh lembaga perbankan untuk memfasilitasi proses identifikasi, verifikasi, dan otorisasi pelanggan. Metode KYC beroperasi mirip dengan CDD, memungkinkan bank untuk memahami klien lebih dalam. Lembaga keuangan diharuskan untuk mengumpulkan informasi dari pelanggan domestik dan internasional, serta entitas nirlaba, bisnis, dan badan pemerintah. Data ini penting untuk melakukan audit keuangan. Namun, besarnya transaksi harian menimbulkan tantangan bagi bank untuk memantau data ini secara efektif dan secara akurat mendeteksi semua aktivitas yang berpotensi penipuan atau transfer yang bisa dipertanyakan.

Pengenalan teknologi elektronik *Know Your Customer* (e-KYC) sangat membantu para profesional kepatuhan dengan memungkinkan lembaga keuangan untuk mengakses informasi pelanggan langsung dari portal pemerintah.<sup>29</sup> Dengan persetujuan pelanggan, lembaga keuangan dapat mengambil dan mengisi detail yang diperlukan dari database yang andal secara otomatis, mengurangi dokumentasi yang ekstensif. Pergeseran ke penggunaan informasi digital ini dapat merampingkan proses orientasi, meminimalisir kesalahan, dan meningkatkan kepatuhan, sehingga dapat menjadi alternatif yang lebih efisien daripada metode KYC konvensional.

<sup>25</sup> AML Law Number 8 Tahun 2010, Art. 23.

<sup>26</sup> AML Law Number 8 Tahun 2010, Art. 23.

<sup>27</sup> Peter Yeoh, "Banks' Vulnerabilities to Money Laundering Activities," *Journal of Money Laundering Control* 23, no. 1 (2019): 122–35, <https://doi.org/10.1108/jmlc-05-2019-0040>

<sup>28</sup> Yeoh.

<sup>29</sup> Yeoh.

Selain e-KYC, sistem peringatan otomatis dapat memberi tahu personel bank dan pelanggan ketika dokumen, seperti KTP, mendekati kedaluwarsanya dan perlu diperbarui. Sistem peringatan otomatis ini membantu lembaga keuangan mempertahankan catatan terkini sambil meningkatkan kepatuhan terhadap peraturan yang berlaku.<sup>30</sup> Dengan mengingatkan pelanggan tentang perpanjangan dokumen secara proaktif, lembaga keuangan dapat mengurangi kasus dokumentasi yang kedaluwarsa dan meminimalkan potensi pelanggaran kepatuhan.

Otomatisasi dalam ekstraksi informasi semakin meningkatkan efektivitas proses KYC, sehingga memungkinkan bank untuk memindai, mengatur, dan mengekstrak informasi yang relevan dari *email* dan dokumen secara efisien. Teknologi ini dapat menghemat waktu dan sumber daya, karena mengurangi jumlah permintaan pemrosesan manual. Namun, efektivitas ekstraksi otomatis bergantung pada tingkat akurasi algoritma yang digunakan.<sup>31</sup> Algoritma yang dirancang dengan buruk dapat menyebabkan kesalahan, memerlukan intervensi manusia tambahan. Oleh karena itu, menjaga presisi algoritma sangat penting untuk optimalisasi.

Sistem AI memiliki kemampuan untuk menelusuri titik data yang banyak, meneliti transaksi yang tampak mencurigakan, dan mengidentifikasi pola yang menunjukkan adanya aktivitas berbahaya.<sup>32</sup> AI, khususnya *computer vision*, memungkinkan bank untuk memverifikasi konsistensi dokumen yang diunggah dengan memeriksa silang informasi yang diberikan pelanggan dengan catatan resmi yang ada.<sup>33</sup> *Computer vision* dapat mendeteksi perbedaan, seperti ketidakcocokan nomor KTP, lalu memberikan peringatan untuk penyelidikan lebih lanjut.<sup>34</sup> Pendekatan berbasis AI ini mendukung jaminan kualitas di semua transaksi, meningkatkan akurasi dan kepercayaan terhadap sistem. Secara keseluruhan, integrasi e-KYC, peringatan otomatis, dan AI meningkatkan proses kepatuhan, mengurangi biaya, dan meningkatkan pengalaman pelanggan.

### ***Beneficial Owner Detection Berbasis AI***

Pencucian uang melibatkan transaksi keuangan lintas Batasan negara sehingga menyulitkan pelacakan sumber dana. Prosesnya terdiri dari serangkaian transaksi untuk menyembunyikan dana ilegal dari pihak berwenang, sehingga menambahkan kesulitan untuk identifikasi pemilik manfaat yang asli. Kompleksitas proses diperparah dengan penggunaan berbagai tingkat dokumentasi data, yang membuatnya sulit untuk mengakses catatan, terutama di berbagai yurisdiksi dan kerangka peraturan. Selain itu, perusahaan dan yayasan dapat menunjuk pemegang saham dan anggota dewan tanpa mengungkapkan identitas pemilik manfaat yang sebenarnya, sehingga semakin menyulitkan proses identifikasi pemilik sah dari dana yang diperoleh secara ilegal.

Kurangnya transparansi perusahaan dan perwalian memungkinkan untuk menyembunyikan identitas pihak yang terlibat dalam kejahatan keuangan, sehingga sulit untuk menuntut pelaku. Implementasi peraturan untuk memerangi pencucian uang telah dilakukan oleh banyak negara dengan mengharuskan perwalian dan perusahaan untuk mendigitalkan daftar mereka dan membuat informasi tentang pemilik manfaat dapat diakses oleh publik.<sup>35</sup>

---

<sup>30</sup> Md. Abdul Hannan et al., “A Systematic Literature Review of Blockchain-Based e-KYC Systems,” *Computing* 105, no. 10 (2023): 2089–2118, <https://doi.org/10.1007/s00607-023-01176-8>.

<sup>31</sup> Hannan et al.

<sup>32</sup> Hannan et al.

<sup>33</sup> Hannan et al.

<sup>34</sup> Hannan et al.

<sup>35</sup> S. Alexandra Bieler, “Peeking into the House of Cards: Money Laundering, Luxury Real Estate, and the Necessity of Data Verification for the Corporate Transparency Act’s Beneficial Ownership Registry,” *Fordham Journal of Corporate and Financial Law* 27 (2022): 193.



Namun, sebagian besar data tidak terstruktur atau dalam catatan tulisan tangan, sehingga sulit untuk memahami informasi dan mengidentifikasi pemilik manfaat.<sup>36</sup>

AI dapat membantu membuat catatan data digital yang terorganisir dan mudah untuk diakses, dengan asumsi bahwa informasi tersebut disertakan dalam pengajuan pemegang saham.<sup>37</sup> AI juga dapat membantu meningkatkan transparansi mengenai kepemilikan manfaat dan memastikan kepatuhan terhadap peraturan yang berlaku, mengurangi resiko organisasi dan eksekutifnya. Pendaftaran pemilik manfaat bersifat wajib dan informasinya harus dapat diakses publik melalui teknologi yang sesuai.

### ***Transactions Monitoring Berbasis AI***

Pemantauan transaksi secara tradisional yang bergantung pada sistem berbasis aturan dapat menghasilkan pemberitahuan berdasarkan skenario yang telah ditentukan sebelumnya. Namun, pendekatan ini memiliki keterbatasan, terutama pada transaksi global dengan skala triliunan. Metode berbasis aturan sering menghasilkan tingkat positif palsu yang tinggi dan akhirnya mengarah pada investigasi yang menggunakan banyak sumber daya. Akibatnya, bank semakin mengadopsi metode pengoptimalan peringatan tingkat lanjut dan mengeksplorasi pemantauan berbasis AI untuk mengelola peringatan dengan lebih efisien.

Salah satu aspek kunci dari pemantauan transaksi adalah penyaringan rekanan secara *real-time*, terutama untuk mencegah dana mencapai entitas yang terkena sanksi. Dalam pembayaran *real-time*, bank harus memverifikasi informasi penerima sebelum persetujuan transaksi untuk memastikan kepatuhan.<sup>38</sup> Jenis penyaringan ini, terutama penyaringan sanksi, sangat penting dalam penyelesaian instan di mana penundaan deteksi dapat memungkinkan dana ilegal ditransfer dan menyebabkan potensi bahaya dan pelanggaran peraturan.<sup>39</sup>

Selain pemantauan secara waktu nyata (*real-time*), tinjauan transaksi terjadwal digunakan untuk mengidentifikasi potensi tindak pidana pencucian uang dengan menilai pola transaksi secara berkala. Bank menetapkan ambang batas tertentu untuk transaksi, seperti penarikan tunai dalam jumlah besar dalam jangka waktu tertentu.<sup>40</sup> Jika suatu transaksi melebihi parameter tersebut, sistem akan memicu peringatan untuk ditindaklanjuti lebih lanjut. Pemantauan terjadwal membantu mendeteksi pola jangka panjang dalam transaksi mencurigakan yang mungkin terlewat oleh pemantauan *real-time*.<sup>41</sup>

*Machine learning* menawarkan solusi untuk mengatasi tantangan dalam memantau transaksi. Algoritme *machine learning* dapat menganalisa pola transaksi, menyesuaikannya dengan tren kejahatan keuangan yang ada, dan menyempurnakan batas peringatan untuk meningkatkan akurasi peringatan.<sup>42</sup> Untuk bank dengan akses terbatas pada model *machine learning*, dapat melakukan penyempurnaan ambang batas, yaitu penyesuaian nilai memicu peringatan, sebagai cara alternatif untuk menyempurnakan sistem pemantauan transaksi dan mengurangi tingkat positif palsu.<sup>43</sup>

Selain itu, matrik tingkat produktivitas membantu dalam mengevaluasi sistem pemantauan. Matrik ini berfokus pada efektivitas peringatan di berbagai tingkatan, mulai dari transaksi hingga perilaku pelanggan tertentu. Selain itu, matrik seperti cakupan SAR, yang melacak proporsi SAR yang ditangkap dalam skenario, dan rasio tumpang tindih yang memantau peringatan multi-skenario untuk pelanggan yang sama, dapat membantu

---

<sup>36</sup> Bieler.

<sup>37</sup> Bieler.

<sup>38</sup> Bieler.

<sup>39</sup> Bieler.

<sup>40</sup> Bieler.

<sup>41</sup> Bieler.

<sup>42</sup> Jullum et al., "Detecting Money Laundering Transactions with Machine Learning."

<sup>43</sup> Jullum et al.

merampingkan investigasi dan memfokuskan sumber daya investigasi pada kasus yang berisiko tinggi.<sup>44</sup>

Segmentasi pelanggan berdasarkan perilaku dan profil risiko adalah langkah dasar dalam penyempurnaan ambang batas. Secara tradisional, segmentasi statis mengelompokkan pelanggan berdasarkan faktor latar belakang, seperti jenis perusahaan atau tingkat eksposur.<sup>45</sup> Namun, segmentasi dinamis menggunakan *unsupervised learning machine learning* memungkinkan pengelompokan yang lebih responsif dan menyelaraskan ambang batas dengan pola transaksi yang berbeda di tiap segmen.<sup>46</sup> Segmentasi dinamis menggunakan *machine learning* membantu mengurangi tingkat positif palsu dan meningkatkan akurasi deteksi aktivitas yang mencurigakan.<sup>47</sup>

Penyempurnaan ambang batas mengikuti pendekatan terstruktur, dimulai dengan menganalisis parameter skenario untuk memastikan ambang batas selaras dengan tujuan bisnis dan peraturan.<sup>48</sup> Ini diikuti dengan mereplikasi logika skenario di lingkungan pengujian untuk menetapkan produktivitas dasar dan cakupan SAR.<sup>49</sup> Menyelesaikan perbedaan secara kolaboratif dengan tim kepatuhan memastikan penyesuaian ambang batas dapat dioptimalkan dan dipahami sebelum diterapkan.

Pengujian di atas garis (*Above-the-line-ATL*) dan di bawah garis (*below-the-line-BTL*) memungkinkan bank untuk menilai tingkat sensitivitas peringatan dengan memodifikasi ambang batas.<sup>50</sup> Ambang batas yang lebih rendah meningkatkan peringatan dan cakupan SAR, sementara ambang batas yang lebih tinggi mengurangi keduanya.<sup>51</sup> Melalui pengujian yang berulang-ulang, bank berusaha memaksimalkan deteksi tanpa membebani sistem dengan positif palsu.<sup>52</sup> Pengoptimalan yang berulang ini sangat penting dalam skenario transaksi frekuensi tinggi, seperti penarikan ATM yang di mana sensitivitas deteksi harus diimbangi dengan efisiensi operasional.

Pengoptimalan dengan berbagai skenario silang meningkatkan pemantauan dengan mengatasi rasio tumpang tindih. Kasus ini bisa terjadi bila ada pelanggan yang memicu beberapa peringatan di berbagai jenis transaksi.<sup>53</sup> Mengurangi tumpang tindih melalui metode pemrograman membantu bank untuk merampingkan investigasi dan memfokuskan sumber daya secara lebih efektif.<sup>54</sup>

Terakhir, menandai perilaku mencurigakan secara akurat sangat penting untuk menyempurnakan tingkat ambang batas. Dengan mendokumentasikan perilaku spesifik yang memicu peringatan, bank dapat meningkatkan sistem pemantauan dan memperkuat kemampuannya untuk menanggapi tren kejahatan keuangan yang terus berkembang. Pendekatan proaktif berbasis data ini pada akhirnya melindungi bank dari risiko peraturan dan meningkatkan kepatuhan sambil memfokuskan sumber daya pada ancaman nyata terhadap integritas keuangan.

<sup>44</sup> Jullum et al.

<sup>45</sup> Guneet Kaur, "Trust the Machine and Embrace Artificial Intelligence (AI) to Combat Money Laundering Activities," in *Disruptive Technologies and Digital Transformations for Society 5.0*, ed. Sandeep Kautish et al. (Singapore: Springer Nature Singapore, 2024), 63–81, [https://doi.org/10.1007/978-981-99-5354-7\\_4](https://doi.org/10.1007/978-981-99-5354-7_4).

<sup>46</sup> Kaur.

<sup>47</sup> Kaur.

<sup>48</sup> Abhishek Gupta, Dwijendra Nath Dwivedi, and Ashish Jain, "Threshold Fine-Tuning of Money Laundering Scenarios through Multi-Dimensional Optimization Techniques," *Journal of Money Laundering Control* 25, no. 1 (2022): 72–78, <https://doi.org/10.1108/jmlc-12-2020-0138>.

<sup>49</sup> Gupta, Dwivedi, and Jain.

<sup>50</sup> Gupta, Dwivedi, and Jain.

<sup>51</sup> Gupta, Dwivedi, and Jain.

<sup>52</sup> Gupta, Dwivedi, and Jain.

<sup>53</sup> Gupta, Dwivedi, and Jain.

<sup>54</sup> Gupta, Dwivedi, and Jain.

## Tantangan Etis

Meskipun AI telah diterima secara positif dalam memerangi kejahatan keuangan, terdapat keterbatasan yang signifikan mempengaruhi tingkat keandalannya. Pelaku kejahatan dapat mengeksploitasi teknologi AI untuk membahayakan keamanan dan integritas sistem keuangan sehingga menciptakan ancaman serius terhadap keamanan digital dan fisik. AI berpotensi menimbulkan bahaya yang signifikan bagi keamanan digital melalui berbagai cara, termasuk memanfaatkan algoritme *machine learning* dan data analitik untuk mengeksploitasi individu yang rentan.<sup>55</sup> AI dapat memperoleh dan menganalisis pola perilaku tertentu yang ditunjukkan oleh pengguna layanan perbankan. Dengan mendapatkan informasi *login* pengguna secara ilegal, AI dapat membuat profil terperinci dari pengguna-pengguna ini yang kemudian dieksploitasi untuk terlibat dalam aktivitas pencucian uang.<sup>56</sup> Serangan *spear-phishing* digunakan untuk memperoleh informasi pribadi penting atau membantu dalam aktivitas penipuan seperti pencurian uang dengan menyamar sebagai entitas pemerintah atau keuangan terkemuka, lalu menipu individu yang tidak menaruh curiga.<sup>57</sup>

Praktik AI yang beretika telah berkembang selama bertahun-tahun, terutama di industri jasa keuangan.<sup>58</sup> Praktik ini menekankan transparansi dengan pedoman yang jelas tentang faktor yang boleh dan tidak boleh digunakan dalam membuat keputusan.<sup>59</sup> Contohnya adalah alat AI Amazon yang bias dalam memberikan iklan di media sosial, biasanya berdasarkan pada budaya pengguna. Hal ini menyoroti potensi AI untuk melakukan kesalahan dan bias dengan cara yang tidak diinginkan atau berbahaya.<sup>60</sup>

Dalam ranah kepatuhan AML, aplikasi AI sering mengandalkan profil untuk mengklasifikasikan demografi tertentu sebagai “berisiko tinggi”.<sup>61</sup> Secara historis, profil yang didasarkan pada faktor demografis dapat menimbulkan kekhawatiran tentang implikasi etisnya. Masalah kuncinya adalah apakah profil semacam itu merupakan bias terhadap kelompok tertentu. Meskipun pembuatan profil dapat berguna dalam mendeteksi potensi risiko, ada sebuah batas yang tipis antara manajemen risiko dan praktik diskriminatif yang secara tidak adil menargetkan komunitas tertentu dan memperkuat kesan berbahaya pada suatu komunitas tertentu.<sup>62</sup>

Masalah privasi adalah tantangan kritis lainnya. Sistem AI sering memproses sejumlah besar data yang tidak terstruktur dan dapat melanggar privasi individu, seperti riwayat transaksi atau interaksi jaringan.<sup>63</sup> Di Indonesia, peraturan privasi masih berkembang, memberikan ketidakpastian tentang bagaimana cara data pribadi harus ditangani. Meskipun belum ada insiden besar yang dilaporkan, risiko AI disalahgunakan untuk mendiskriminasi pelanggan tetap menjadi perhatian yang nyata.

<sup>55</sup> Abhishek Gupta, Dwijendra Nath Dwivedi, and Jigar Shah, *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance*, Future of Business and Finance (Singapore: Springer Nature Singapore, 2023), <https://doi.org/10.1007/978-981-99-2571-1>.

<sup>56</sup> Gupta, Dwivedi, and Shah.

<sup>57</sup> Gupta, Dwivedi, and Shah.

<sup>58</sup> Faraz Ahmed, “Ethical Aspects of Artificial Intelligence in Banking,” *Journal of Research in Economics and Finance Management* 1, no. 2 (2022): 55–63, <https://doi.org/10.56596/jrefm.v1i2.7>.

<sup>59</sup> Ahmed.

<sup>60</sup> Ahmed.

<sup>61</sup> Sheshadri Chatterjee and N. S. Sreenivasulu, “Artificial Intelligence and Human Rights: A Comprehensive Study from Indian Legal and Policy Perspective,” *International Journal of Law and Management* 64, no. 1 (2022): 110–34, <https://doi.org/10.1108/ijlma-02-2021-0049>.

<sup>62</sup> Chatterjee and Sreenivasulu.

<sup>63</sup> Sinta Dewi and Mohammad Wildan Hidayat, “Protection of Data Privacy in the Era of Artificial Intelligence in the Financial Sector in Indonesia,” *Journal of Central Banking Law and Institutions* 1, no. 2 (2022): 353–66, <https://doi.org/10.21098/jcli.v1i2.18>.

Sistem AI juga rentan terhadap berbagai jenis bias yang bisa dimasukkan melalui keputusan manusia, pemilihan data, dan desain model.<sup>64</sup> Bias dari manusia sering memengaruhi perkembangan sistem AI, baik secara sadar maupun tidak sadar. Bias ini dapat didasarkan pada pengalaman masa lalu atau prasangka tentang demografis tertentu.<sup>65</sup> Misalnya, pembuat keputusan dapat mengasosiasikan profesi tertentu dengan perilaku tertentu, dan ini dapat memengaruhi data yang dipilih untuk melatih model AI.<sup>66</sup> Bias berbasis data adalah sumber kesalahan AI lainnya. Data yang diklasifikasikan dengan buruk atau salah direpresentasikan dapat menyebabkan hasil yang kurang baik.<sup>67</sup> Dalam proses KYC, bias dapat secara tidak proporsional mempengaruhi kelompok tertentu, yang menyebabkan perlakuan yang tidak adil. Misalnya, sistem AI mungkin menandai kelompok tertentu sebagai berisiko tinggi berdasarkan pola historis, tetapi pola ini mungkin tidak mencerminkan realitas saat ini.

Seiring dengan semakin canggihnya AI, penting untuk memastikan bahwa standar etika juga ikut berkembang untuk melindungi kepercayaan pelanggan dan memastikan stabilitas pasar keuangan. Meskipun algoritma AI dapat mengungguli manusia dalam memproses data, mereka sering membenarkan bias manusia, kecuali bila ada tindakan pencegahan yang diterapkan.<sup>68</sup> Penggunaan *Big Data* dalam analisis AI dapat melanggar privasi, yang mengancam hak asasi manusia.

AI telah memperkenalkan risiko yang signifikan terhadap HAM, memperburuk masalah yang ada, dan menciptakan tantangan baru dalam berbagai bidang seperti pengambilan keputusan algoritmik.<sup>69</sup> Model statistik tradisional memang cenderung lebih mudah dan tidak berdampak pada HAM, namun proses pengambilan keputusan AI yang kompleks dapat secara tidak sengaja melanggar HAM dengan membenarkan bias, seperti dalam peradilan pidana, ketenagakerjaan, dan pengawasan.<sup>70</sup> Sistem AI juga dapat menyebabkan diskriminasi, informasi yang salah, dan perlakuan yang tidak setara. Pada akhirnya, ini bisa mempengaruhi kelompok rentan secara tidak proporsional.<sup>71</sup> Risiko ini menimbulkan perhatian tentang potensi ketidakseimbangan kekuasaan dan bagaimana AI dapat memperkuat penindasan. Mengatasi masalah ini melalui perlindungan hak asasi manusia yang efektif dirasa sangat penting.

Undang-undang HAM memiliki peran penting dalam mengurangi bahaya yang disebabkan oleh AI, tetapi menentukan dampak "baik" dan "buruk" dari AI itu kompleks dan membutuhkan pertimbangan etis. Prinsip-prinsip etika seperti keadilan, akuntabilitas, dan transparansi dapat memandu pengembangan dan penggunaan teknologi AI dan membantu menentukan batasan antara praktik yang dapat diterima atau termasuk berbahaya. Perusahaan teknologi seperti Microsoft, IBM, dan Google telah mengembangkan pedoman etika AI mereka sendiri, meskipun prinsip-prinsip ini tidak selalu didefinisikan secara jelas.<sup>72</sup> Namun demikian, prinsip-prinsip HAM diakui secara universal dan memberikan dasar untuk meminta pertanggungjawaban sistem AI. Ketika AI dianggap tidak etis, itu tidak hanya melanggar hak individu tetapi juga merusak prinsip-prinsip inti hukum HAM.

## Kerangka Kerja Global

Norma dan peraturan internasional yang mengatur bidang tertentu juga memiliki tingkat universalitas. Misalnya Pedoman Etika Masyarakat Jepang untuk Kecerdasan Buatan yang

---

<sup>64</sup> Chatterjee and Sreenivasulu, "Artificial Intelligence and Human Rights."

<sup>65</sup> Chatterjee and Sreenivasulu.

<sup>66</sup> Chatterjee and Sreenivasulu.

<sup>67</sup> Chatterjee and Sreenivasulu.

<sup>68</sup> Chatterjee and Sreenivasulu.

<sup>69</sup> Chatterjee and Sreenivasulu.

<sup>70</sup> Chatterjee and Sreenivasulu.

<sup>71</sup> Chatterjee and Sreenivasulu.

<sup>72</sup> Morgan Sullivan, "Big Tech's Evolving Role in AI Governance: Shaping Ethical Standards," *Transcend*, March 21, 2024, <https://transcend.io/blog/big-tech-ai-governance>.

merekomendasikan audit algoritma yang dibuat oleh pemerintah.<sup>73</sup> Gagasan ini memiliki daya tarik dan akhirnya diadopsi oleh Komite Intelijen Senat AS sebagai sarana untuk mempromosikan pengambilan keputusan yang adil dan tidak bias.<sup>74</sup>

GDPR Uni Eropa juga dirancang untuk melindungi privasi data bagi individu di dalam Uni Eropa, memperluas pengaruhnya ke organisasi mana pun yang menangani data tentang warga negara Uni Eropa.<sup>75</sup> Beberapa organisasi seperti *Organisation for Economic Co-operation and Development* (OECD) dan *European Union's Artificial Intelligence High-Level Expert Group* (AI HLEG) bekerja sama dengan badan-badan regional untuk mengembangkan prinsip-prinsip yang membantu membuat sistem AI yang dapat dipercaya dan etis.<sup>76</sup> Keduanya telah mengajukan pedoman yang menyoroti beberapa nilai penting seperti transparansi, akuntabilitas, privasi, dan dampak sosial AI yang lebih luas.<sup>77</sup> Pedoman OECD menggarisbawahi perlunya AI untuk mendukung pertumbuhan yang inklusif, keberlanjutan, dan sejahtera.<sup>78</sup> Namun, prinsip-prinsip ini umumnya bersifat tingkat tinggi dan tidak memberikan panduan teknis secara khusus sehingga menyisakan ruang untuk interpretasi dan evolusi seiring kemajuan AI.

Salah satu prinsip utama OECD adalah transparansi seputar sistem AI, menekankan betapa pentingnya agar pengguna bisa menantang keputusan berbasis AI.<sup>79</sup> Di sektor-sektor seperti AML, transparansi tidak selalu berarti memberi tahu individu yang ditandai, melainkan model AI harus dapat dimengerti dan dijelaskan oleh badan pengawas sehingga memungkinkan pengawasan yang tepat terhadap algoritme yang digunakan. Persyaratan ini juga terkait dengan kebutuhan akan hasil yang dapat direproduksi dan handal (*input* serupa akan menghasilkan *output* yang konsisten), memperkuat keandalan sistem AI dalam aplikasi berisiko tinggi ini.

Keamanan dan evaluasi risiko berkelanjutan adalah titik fokus lainnya yang ditekankan dalam Prinsip 4 dari OECD.<sup>80</sup> Sistem AI diharapkan dapat beroperasi dengan aman, bahkan dalam kondisi yang menantang atau tidak terduga. Prinsip ini sejalan dengan pendekatan berbasis risiko UE terhadap regulasi AI, yang saat ini ditetapkan dalam Undang-Undang AI yang diusulkan.<sup>81</sup> Undang-undang yang diluncurkan pada April 2022 bertujuan untuk menetapkan standar AI yang dapat ditegakkan di seluruh UE, menangani bidang-bidang seperti transparansi, pengawasan manusia, perlindungan data, dan keamanan siber. Undang-undang tersebut mencakup kerangka kerja risiko berjenjang, di mana aplikasi berisiko tinggi seperti perangkat medis dan AI untuk proses perekrutan menjalani evaluasi yang ketat, sementara aplikasi berisiko rendah seperti *chatbot* mengharuskan pengguna untuk diberitahu bahwa mereka berinteraksi dengan AI.<sup>82</sup> Pendekatan ini berupaya menyeimbangkan pengawasan peraturan dengan fleksibilitas yang diperlukan untuk mendorong inovasi dalam AI, meminimalisir beban peraturan untuk teknologi berisiko rendah.

---

<sup>73</sup> Japanese Society for Artificial Intelligence, "The Japanese Society for Artificial Intelligence Ethical Guidelines," Japanese Society for Artificial Intelligence, last modified 2017, <https://www.ai-gakkai.or.jp/ai-elsi/wp-content/uploads/sites/19/2017/05/JSAI-Ethical-Guidelines-1.pdf>.

<sup>74</sup> The Senate of The United States, "Bill to Provide a Framework for Artificial Intelligence Innovation and Accountability, and for Other Purposes," congress.gov, last modified November 15, 2023, <https://www.congress.gov/118/bills/s3312/BILLS-118s3312is.pdf>.

<sup>75</sup> The European Parliament and The Council, 2016/679 *General Data Protection Regulation* (The European Parliament and The Council, 2016).

<sup>76</sup> Alexandru Circiumaru, "Towards European AI: Part I - Setting the Context," Queen Mary University of London, last modified October 18, 2019, <https://www.qmul.ac.uk/euplant/blog/items/towards-european-ai-part-i---setting-the-context-.html>.

<sup>77</sup> Circiumaru.

<sup>78</sup> OECD, "AI Principles," OECD, last modified 2024, <https://www.oecd.org/en/topics/sub-issues/ai-principles.html>.

<sup>79</sup> OECD.

<sup>80</sup> OECD.

<sup>81</sup> Circiumaru, "Towards European AI."

<sup>82</sup> Circiumaru.

Undang-Undang AI UE merupakan langkah yang penting karena memperkenalkan peraturan yang dapat ditegakkan yang berlaku untuk aplikasi AI dalam pasar tunggal digital.<sup>83</sup> Bila banyak negara anggota UE juga mendukung pedoman FATF dan OECD, Undang-Undang AI akan melangkah lebih jauh dengan menetapkan aturan wajib untuk semua teknologi AI, terutama yang berada di sektor berisiko tinggi seperti AML. Di bidang ini, AI memiliki peran penting dalam menganalisis kumpulan data yang luas untuk mendeteksi aktivitas kriminal.<sup>84</sup> Dengan keterlibatan AI, upaya AML akan mendapatkan keunggulan analitis, memungkinkan tim untuk fokus pada kasus berisiko tinggi sementara AI menangani pekerjaan awal seperti agregasi data.

Undang-Undang AI UE mengamanatkan pengawasan manusia yang berkelanjutan untuk aplikasi AI berisiko tinggi di AML, memastikan bahwa *operator* dapat menghentikan atau meninjau keputusan otomatis kapan saja.<sup>85</sup> Pengawasan manusia yang berkelanjutan untuk aplikasi AI berisiko tinggi mendukung prinsip penjelasan model, yang memungkinkan pengguna untuk memahami bagaimana dan mengapa sistem AI memberikan hasil tertentu. Ini merupakan fitur penting untuk mendeteksi potensi bias atau kesalahan. Untuk mematuhi, entitas yang diatur harus menerapkan protokol keamanan data yang kuat, memelihara jejak audit terperinci, dan menetapkan kerangka kerja tata kelola yang mungkin mencakup peran baru seperti petugas kepatuhan AI. Meskipun transisi ini menghadirkan tantangan praktis, hal ini secara luas dipandang sebagai langkah penting untuk membangun kepercayaan publik dan memastikan bahwa AI diterapkan secara etis dan bertanggung jawab dalam wilayah yang kritis seperti pencegahan kejahatan keuangan.

Undang-Undang AI UE adalah langkah substansial menuju harmonisasi regulasi AI, menetapkan tolok ukur global yang dapat mempengaruhi standar AI di seluruh dunia.<sup>86</sup> Seiring berjalannya implementasi, fokusnya akan tetap pada pembinaan keseimbangan antara inovasi dan pengawasan, memastikan AI membantu umat manusia dengan cara yang transparan, adil, dan bertanggung jawab.

Hukum membutuhkan keseimbangan yang harmonis antara menjaga HAM dan memberlakukan pembatasan secara proporsional. Oleh karena itu, klausul pembatasan harus digunakan sebagai kriteria untuk mengatasi tantangan prosedur AML berbasis AI. Tes proporsionalitas adalah metode yang umum digunakan dalam masyarakat demokratis untuk membatasi hak.<sup>87</sup>

Tes proporsionalitas adalah prinsip hukum konstitusional yang digunakan secara luas dalam masyarakat demokratis, berfungsi untuk mencapai keseimbangan antara hak-hak individu dan pembatasan hukum yang berlaku. Hukum tata negara umum mengacu pada prinsip-prinsip dasar, teori, praktik, dan doktrin hukum tata negara yang berlaku secara luas, tanpa terikat pada yurisdiksi tertentu.<sup>88</sup> Ini menunjukkan bahwa ketika pendekatan, praktik, atau prinsip telah digunakan secara konsisten di berbagai yurisdiksi dapat mencapai status hukum konstitusional umum. Pemeriksaan telah diterapkan di berbagai yurisdiksi yang mematuhi sistem hukum perdata dan umum.<sup>89</sup>

Selain itu, uji ini juga telah diterapkan oleh pengadilan HAM regional, termasuk *European Court of Human Rights*, *Inter-American Court of Human Rights*, dan *European Court of*

---

<sup>83</sup> Circiumaru.

<sup>84</sup> Circiumaru.

<sup>85</sup> Circiumaru.

<sup>86</sup> Circiumaru.

<sup>87</sup> Circiumaru.

<sup>88</sup> Circiumaru.

<sup>89</sup> Circiumaru.

*Justice*.<sup>90</sup> Prinsip yang mendasari uji proporsionalitas adalah untuk mencapai keseimbangan yang harmonis antara metode yang digunakan dan hasilnya.<sup>91</sup> Ketika mempertimbangkan keseimbangan antara bentuk dan hasil akhir, sarana yang digunakan harus bermanfaat, esensial, cocok, dan proporsional. Dalam karyanya, Bernhard Schlink memberikan anekdot ilustratif dengan seorang penyandang disabilitas yang berusaha melindungi propertinya, yaitu koleksi apel, dari seorang anak yang suka mencuri.<sup>92</sup> Anak tersebut menunjukkan kurangnya kepatuhan pada instruksi lisan untuk menahan diri dan tidak mengambil apelnya. Satu-satunya metode yang tersedia bagi Schlink adalah dengan melibatkan penggunaan senjata api untuk melepaskan proyektil untuk membahayakan anak itu. Dalam hal ini, Schlink menjelaskan efektifitas dan perlunya menggunakan kekuatan yang mematikan untuk melindungi apel yang dianggap sebagai miliknya<sup>93</sup>.

Namun, menembak seorang anak untuk mempertahankan apel dianggap salah atau tidak seimbang secara moral karena perbedaan yang melekat antara nyawa anak dan nilai yang relatif sepele dari apel. Schlink menawarkan contoh spesifik dari kasus di hadapan Mahkamah Konstitusi Federal Jerman.<sup>94</sup> Pengadilan mengajukan pertanyaan mengenai izinnya ekstraksi cairan serebrospinal terdakwa oleh negara untuk menilai kemampuan kognitif mereka.<sup>95</sup> Pengadilan memberikan keputusan yang menegaskan legitimasi tujuan untuk memastikan kemampuan mental. Namun, pengadilan mengakui ketidaknyamanan dan risiko yang terlibat dalam proses ekstraksi. Akibatnya, pengadilan memutuskan bahwa ekstraksi tersebut hanya dibenarkan dalam kasus dengan tingkat keparahan yang substansial.

Potensi pembatasan HAM secara eksplisit diuraikan dalam Pasal 29 *Universal Declaration of Human Rights* (UDHR), yang menegaskan:

*"The exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order, and the general welfare in a democratic society."*<sup>96</sup>

"Dalam pelaksanaan hak dan kebebasannya, setiap orang hanya akan tunduk pada batasan yang ditentukan oleh hukum semata-mata untuk mengamankan pengakuan dan penghormatan yang semestinya terhadap hak dan kebebasan orang lain dan untuk memenuhi persyaratan moralitas, ketertiban umum, dan kesejahteraan umum yang adil dalam masyarakat demokratis."

## Kompatibilitas dengan Hukum HAM di Indonesia

Di Indonesia, masih belum ada regulasi tentang pemanfaatan AI. Sistem hukum Indonesia menyarankan untuk mengatur regulasi AI yang prospektif dan kompatibilitas HAM dengan menentukan prinsip AI yang bertanggung jawab. Prinsip-prinsip hukum ini akan menjadi pedoman untuk mencegah bahaya dan risiko teknologi AI dan untuk memperkuat upaya pencegahan pencucian uang.

---

<sup>90</sup> Emil Śliwiński, "Principle of Proportionality as a Threat to Criminal-Law-Related Fundamental Rights," *New Journal of European Criminal Law* 14, no. 3 (2023): 327–44, <https://doi.org/10.1177/20322844231158323>.

<sup>91</sup> Śliwiński.

<sup>92</sup> Bernhard Schlink, "Proportionality in Constitutional Law: Why Everywhere but Here?," *Duke Journal of Comparative & International Law* 22 (2012): 291.

<sup>93</sup> Schlink.

<sup>94</sup> Schlink.

<sup>95</sup> Schlink.

<sup>96</sup> United Nations, "Universal Declaration of Human Rights," United Nations, last modified 1948, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

Tidak diragukan lagi, HAM dan hak lainnya tunduk pada suatu batasan.<sup>97</sup> Jadi, perlu diselidiki potensi pemanfaatan UUD 1945 dan UU AML Indonesia untuk mengatasi dilema tersebut. Pasal 28 J tahun 1945 dengan nada yang sebanding dengan Pasal 29 UDHR menunjukkan ketentuan pembatasan dalam Konstitusi 1945. Ketentuan pembatasan yang diuraikan dalam Pasal 28J UUD 1945 menyebutkan:

"Dalam menjalankan hak dan kebebasan, setiap orang harus tunduk pada batasan yang ditentukan oleh hukum semata-mata untuk mengamankan pengakuan dan penghormatan terhadap hak dan kebebasan orang lain dan untuk memenuhi persyaratan moralitas, nilai-nilai agama, keamanan, ketertiban umum, dalam masyarakat yang demokratis."<sup>98</sup>

Gagasan perlunya pembatasan tertentu terhadap HAM didukung oleh Mahkamah Konstitusi Indonesia (MK). Dalam putusan pengadilan nomor 14/PUU-VI/2008, MK mengakui bahwa, terkadang pembatasan hak tidak dapat dihindari, bahkan ketika UUD 1945 tidak menyertakan klausul pembatasan eksplisit.<sup>99</sup>

Dalam hal ini, uji proporsionalitas memastikan bahwa kekuasaan pemerintah yang diberikan oleh undang-undang tertentu tidak secara berlebihan melanggar hak-hak dasar, seperti hak atas privasi, non-diskriminasi, pengadilan yang adil, atau kebebasan berekspresi. Penerapan uji proporsionalitas diamati dalam dua konteks yang berbeda dalam kerangka hukum Indonesia. Pertama, digunakan sebagai persyaratan proporsionalitas yang ditetapkan dalam konstitusi.<sup>100</sup> Kedua, digunakan sebagai persyaratan proporsionalitas undang-undang yang ditemukan dalam hukum nasional.<sup>101</sup>

Terlepas dari apakah undang-undang tersebut secara eksplisit menyebutkan proporsionalitas, gagasan proporsionalitas tertanam dalam kerangka undang-undang.<sup>102</sup> Undang-undang yang gagal mematuhi prinsip proporsionalitas di tingkat konstitusional dianggap batal dalam hukum.<sup>103</sup> Salah satu ketentuan yang paling relevan untuk AML adalah Pasal 26 UU No. 19/2016 tentang Informasi dan Transaksi Elektronik, yang melindungi hak privasi.

Uji proporsionalitas terdiri dari tiga langkah berurutan yang harus dipenuhi secara kolektif. Tahap awal melibatkan analisis apakah suatu kebijakan telah ditetapkan berdasarkan undang-undang atau peraturan yang spesifik, dapat dipahami, dan telah diberlakukan dengan prosedur demokratis.<sup>104</sup> Langkah kedua melibatkan evaluasi apakah kebijakan yang dimaksud selaras dengan tujuan yang valid, seperti melindungi hak-hak dasar atau mengatasi masalah sosial yang signifikan.<sup>105</sup> Fase ketiga adalah menanyakan tentang perlunya tindakan dalam konteks masyarakat demokratis.<sup>106</sup> Fase ketiga memiliki tingkat kesulitan yang paling signifikan dan mencakup beberapa tes lanjutan. Tes lanjutan ini menilai efektivitas ukuran, tingkat intrusifnya dibandingkan dengan standar lain yang ada, keseimbangan yang adil antara hak-hak yang terlibat, dan perlindungan yang memadai.

Tahap pertama dari uji proporsionalitas, sebagaimana disyaratkan oleh hukum, menuntut agar setiap tindakan pembatasan hak didefinisikan dengan jelas dalam undang-undang.

---

<sup>97</sup> Schlink, "Proportionality in Constitutional Law."

<sup>98</sup> Constitutional Court of the Republic of Indonesia, "The 1945 Constitution of the Republic of Indonesia," MKRI, last modified 2020, <https://en.mkri.id/library/constitution>.

<sup>99</sup> Constitutional Court of the Republic of Indonesia, "Decision Number 14/PUU-VI/2008," MKRI 2020, <https://en.mkri.id/court/decision?search=14%2FPUU-VI%2F2008>.

<sup>100</sup> Jan Sieckmann, "Proportionality as a Universal Human Rights Principle," in *Proportionality in Law*, ed. David Duarte and Jorge Silva Sampaio (Cham: Springer International Publishing, 2018), 3–24, [https://doi.org/10.1007/978-3-319-89647-2\\_1](https://doi.org/10.1007/978-3-319-89647-2_1).

<sup>101</sup> Sieckmann.

<sup>102</sup> Sieckmann.

<sup>103</sup> Sieckmann.

<sup>104</sup> Sieckmann.

<sup>105</sup> Sieckmann.

<sup>106</sup> Sieckmann.



Undang-undang ini harus menentukan fitur teknologi yang digunakan, jenis data yang diproses, dan pengamanan yang ada. Kejelasan seperti itu memungkinkan warga negara dan pemangku kepentingan politik untuk memahami langkah, menilai implikasi, dan meminta pertanggungjawaban pemerintah atas implementasinya.<sup>107</sup> Terdapat fleksibilitas yang signifikan dalam menafsirkan peraturan AML mengenai pemantauan transaksi. Ketentuan ini memerlukan sistem untuk menunjukkan keefektifan dalam menghalangi pembayaran yang ditujukan kepada entitas yang dikenakan sanksi internasional.<sup>108</sup> Selain itu, sistem harus dirancang untuk mengidentifikasi transaksi yang mencurigakan dengan mempertimbangkan skenario risiko yang ditentukan dengan cermat.

Secara praktis, badan pengatur mengantisipasi bahwa bank akan mematuhi standar industri saat menerapkan sistem. Standar ini tunduk pada pengembangan berkelanjutan karena vendor teknologi AML memperkenalkan prosedur yang semakin canggih dan invasif. Perlu dicatat bahwa kerangka hukum tidak menetapkan batas atas yang eksplisit dalam hal ini. Lintasan ke atas ini didorong oleh persepsi bank bahwa meningkatkan investasi dalam teknologi dan personel kepatuhan akan mengurangi kemungkinan pelanggaran peraturan. Bank cenderung menganggap sanksi AML, yang bisa mencakup seperti pembatalan lisensi perbankan, sebagai risiko yang lebih konsekuensial daripada risiko perlindungan data. Gagasan ini dapat menyebabkan bank melakukan kesalahan dalam menggunakan sistem kepatuhan yang lebih canggih.

Elemen proporsionalitas kedua yang melibatkan tujuan yang valid dan mengatasi kebutuhan sosial yang mendesak, dapat dengan mudah dipenuhi dalam kasus strategi AML. Strategi AML secara inheren terkait dengan upaya yang lebih luas untuk memerangi kegiatan kriminal yang berat dan terorisme. Pasal 26 UU No. 19 Tahun 2016 secara eksplisit menyatakan bahwa ada alasan yang sah untuk melanggar hak privasi, termasuk kasus-kasus yang berkaitan dengan AML, asalkan campur tangan tersebut proporsional.

Prinsip Siracusa memperhatikan masalah pelecehan pemerintah yang meluas dalam menggunakan klausul pembatasan HAM untuk membatasi HAM secara sepihak. Terdapat sembilan prinsip utama untuk memandu bagaimana negara dapat secara hukum memberlakukan pembatasan HAM menggunakan klausul pembatasan.<sup>109</sup> Pada prinsipnya, ini menggarisbawahi elemen-elemen penting yang terlibat dalam pembatasan hak. Istilah "perlu" menunjukkan bahwa pembatasan dan persyaratan lainnya harus sepadan dengan tujuannya.<sup>110</sup>

Dokumen penting lainnya, Komentar Umum No. 31 (2004) dari Komisi Hak Asasi Manusia, menjelaskan bahwa negara-negara harus membenarkan setiap pembatasan hak berdasarkan Kovenan Internasional tentang Hak-hak Sipil dan Politik (ICCPR).<sup>111</sup> Ia menyatakan bahwa pembatasan ini harus diperlukan dan proporsional dengan tujuan sah yang ingin mereka capai, memastikan bahwa hak-hak yang dilindungi oleh Kovenan tetap dilindungi secara efektif.<sup>112</sup>

Komponen penting dari tahap proporsionalitas ketiga memerlukan evaluasi sejauh mana teknik tertentu benar-benar efektif dalam mencapai tujuan yang diinginkan sementara juga menjadi cara paling invasif yang tersedia.<sup>113</sup> Namun, metodologi apa yang dapat digunakan

---

<sup>107</sup> Sieckmann.

<sup>108</sup> Sieckmann.

<sup>109</sup> Alex Conte, "Limiting Rights Under International Law," in *Human Rights in the Prevention and Punishment of Terrorism*, ed. Alex Conte (Berlin, Heidelberg: Springer Berlin Heidelberg, 2010), 283–314, [https://doi.org/10.1007/978-3-642-11608-7\\_10](https://doi.org/10.1007/978-3-642-11608-7_10).

<sup>110</sup> Conte.

<sup>111</sup> UN Human Rights Committee, "General Comment No. 31 [80], the Nature of the General Legal Obligation Imposed on States Parties to the Covenant," Refworld, last modified May 26, 2004, <https://www.refworld.org/legal/general/hrc/2004/en/52451>.

<sup>112</sup> UN Human Rights Committee.

<sup>113</sup> Schlink, "Proportionality in Constitutional Law."

untuk menilai kemandirian strategi AML? Seperti yang dikatakan sebelumnya, bank menetapkan kesuksesan mereka semata-mata dengan mengandalkan laporan sejarah. Dalam konteks perbankan, kemandirian peringatan meningkat ketika memiliki kemiripan dengan skenario yang sebelumnya telah diidentifikasi oleh tim kepatuhan bank sebagai bermasalah. Namun, lembaga keuangan kurang mengetahui tentang efektivitas laporan aktivitas mencurigakan mereka dalam memfasilitasi upaya penegakan hukum. Konfirmasi atau penolakan potensi hubungan antara aktivitas mencurigakan yang diamati oleh bank dan perilaku kriminal saat ini ditahan oleh otoritas penegak hukum.

Salah satu aspek yang penting adalah transparansi, di mana orang harus diberitahu tentang identifikasi mereka sebagai ancaman potensial untuk terlibat dalam tindakan ilegal.<sup>114</sup> Namun demikian, undang-undang tentang AML membatasi tindakan tersebut karena potensi kompromi investigasi kriminal yang mungkin timbul dari pemberitahuan tersebut. Masalah mengkomunikasikan aktivitas pengawasan secara efektif kepada subjek yang dipantau menimbulkan tantangan yang signifikan bagi berbagai sistem pengawasan, terutama yang digunakan dalam keamanan nasional dan operasi anti-terorisme, ketika kerahasiaan sangat penting. Sikap yang diadopsi oleh pengadilan adalah bahwa orang harus segera diberitahu sambil memastikan bahwa pemberitahuan tersebut tidak membahayakan penyelidikan yang sedang berlangsung. Proposal ini mengemukakan bahwa ada kebutuhan untuk mengubah undang-undang AML untuk memberikan bank kemampuan untuk memberi tahu pelanggan yang telah menjadi subjek SAR pada titik waktu tertentu setelah transmisi SAR ke FIU kecuali FIU secara eksplisit menentukan bahwa pemberitahuan tersebut akan menghambat penyelidikan yang sedang berlangsung. Otoritas penegak hukum menanggung beban membuktikan bahwa memberi tahu pelanggan tertentu akan membahayakan penyelidikan yang sedang berlangsung. Menyembunyikan informasi tersebut secara permanen, terutama ketika SAR tidak pernah ditindaklanjuti, tampaknya tidak adil.

Uji proporsionalitas menetapkan bahwa setiap pelanggaran terhadap hak pribadi atau pembatasan hak lainnya harus mematuhi prinsip proporsionalitas.<sup>115</sup> Oleh karena itu, sangat penting untuk menetapkan peraturan dalam kerangka intervensi pemerintah. Ketika dihadapkan dengan pertanyaan tentang pemantauan transaksi, langkah awal akan melibatkan penilaian sejauh mana HAM terpengaruh. Metode deteksi AML pada dasarnya mengganggu karena mencakup analisis komprehensif data transaksi dari semua klien, terlepas dari keberadaan teknik *machine learning*.

## Rekomendasi Kebijakan

Regulasi dari risiko yang sistemik terkait dengan strategi AML berbasis AI menyoroti bidang-bidang penting yang perlu diperhatikan untuk memastikan perlindungan HAM, terutama dalam tata kelola, akuntabilitas, dan etika.<sup>116</sup> Upaya peraturan saat ini berfokus untuk memastikan bahwa lembaga keuangan dan pengembang AI mempertahankan kontrol internal yang kuat untuk memantau dan mengelola risiko di seluruh siklus hidup pengembangan AI.<sup>117</sup> Kunci dari kontrol ini adalah prinsip akuntabilitas bersama, di mana pengembang dan pengguna bertanggung jawab atas risiko sistemik yang ditimbulkan oleh teknologi AI.<sup>118</sup> Akuntabilitas ini harus ditegakkan pada tingkat tertinggi untuk aplikasi AI dengan implikasi keuangan yang signifikan, memastikan bahwa pengawasan manusia tetap utuh. Transparansi dalam proses

---

<sup>114</sup> Schlink.

<sup>115</sup> Conte, "Limiting Rights Under International Law."

<sup>116</sup> Ondrej Bajgar and Jan Horenovsky, "Negative Human Rights as a Basis for Long-Term AI Safety and Regulation," *Journal of Artificial Intelligence Research* 76 (2023): 1043–75, <https://doi.org/10.1613/jair.1.14020>.

<sup>117</sup> Bajgar and Horenovsky.

<sup>118</sup> Bajgar and Horenovsky.

pengambilan keputusan sistem AI sangat penting sehingga sistem ini dapat dijelaskan dan dikendalikan oleh operator manusia bila diperlukan.

Meskipun upaya regulasi ini merupakan dasar yang kuat untuk mengelola risiko AI di industri perbankan, hal ini sangat bergantung pada kesiapan dan akuntabilitas pengembang AI dan bank. Agar regulasi menjadi efektif, bank harus memiliki kemampuan untuk memantau dan menjelaskan perilaku AI secara handal. Untuk mencapai hal ini, regulator harus melibatkan personel yang terampil dalam mengembangkan atau memperoleh teknologi terkait AI serta memungkinkan mereka memverifikasi fungsionalitas sistem AI secara mandiri. Kompleksitas AI, dikombinasikan dengan kebutuhan akan keterampilan khusus, membuat keterlibatan regulasi penuh menjadi tantangan terutama dalam kasus sistem AI dengan potensi kepentingan sistemik. Akibatnya, regulator mungkin merasa lebih layak untuk memfokuskan upaya mereka pada kasus-kasus berisiko tinggi, di mana potensi dampaknya paling besar terhadap stabilitas keuangan.

Fleksibilitas dan kemampuan beradaptasi adalah inti dari regulasi AI, terutama mengingat laju kemajuan AI yang cepat dan kesenjangan informasi yang sering ada di antara regulator dan pasar.<sup>119</sup> Tes proporsionalitas mengakui perlunya kerangka hukum yang dapat berkembang seiring dengan perkembangan teknologi. Fleksibilitas ini tidak boleh mengarah pada kekosongan peraturan, di mana sistem AI beroperasi tanpa pengawasan yang memadai. Pendekatan peraturan berbasis risiko menawarkan solusi yang seimbang dengan menetapkan pedoman luas yang memprioritaskan privasi data, perlindungan konsumen, dan langkah-langkah keamanan. Pendekatan semacam itu memberikan perimeter peraturan yang stabil sambil memungkinkan penyesuaian yang diperlukan untuk mengatasi risiko yang muncul.

Peraturan harus mewajibkan fitur yang memungkinkan sistem dinonaktifkan jika sistem mulai beroperasi di luar batas agar menjaga kendali manusia pada teknologi AI.<sup>120</sup> Selain itu, kerangka peraturan yang lebih jelas diperlukan untuk menentukan persyaratan kepatuhan bagi pengembang AI dan bank, karena hukum seputar regulasi AI saat ini sedang berkembang. Dengan menetapkan standar yang konkrit, regulator dapat membantu mencegah ambiguitas yang dapat menyebabkan praktik kepatuhan yang tidak konsisten atau celah dalam manajemen risiko AI.

Tantangan bagi regulator diperburuk oleh laju perkembangan pasar yang lebih cepat dari implementasi peraturan. Meskipun kesenjangan ini umumnya diterima sebagai bagian dari dinamika pasar, hal ini dapat menimbulkan risiko parah terhadap stabilitas keuangan jika regulator tidak siap untuk menanggapi masalah terkait AI yang sistemik. Regulator harus tetap mendapat informasi tentang kemajuan AI yang cepat untuk mengurangi penundaan antara pengembangan AI dan respons peraturan. Berinvestasi dalam teknologi AI itu sendiri dapat meningkatkan kapasitas regulator untuk memantau perkembangan secara *real time* sehingga dapat menawarkan cara untuk menjembatani kesenjangan informasi dan mengantisipasi potensi masalah dengan lebih baik.<sup>121</sup>

Dalam konteks deteksi AML, regulator mungkin memerlukan kekuatan yang lebih luas untuk merespons dengan cepat dan efektif. Karena tantangan terkait AI dapat secara signifikan memengaruhi hak-hak individu, kerangka peraturan harus cukup fleksibel untuk memungkinkan intervensi secara tepat waktu. Pergeseran ini juga dapat membentuk kembali lanskap peraturan serta berpotensi mengurangi peran sistem hukum dan pengadilan tradisional karena regulator mengambil peran yang lebih sentral dalam mengelola keadaan darurat terkait AI. Sikap regulasi yang proaktif dengan kekuatan darurat yang cukup akan memungkinkan

---

<sup>119</sup> Alberto Quintavalla and Jeroen Temperman, *Artificial Intelligence and Human Rights* (Oxford, UK: Oxford University Press, 2023).

<sup>120</sup> Quintavalla and Temperman.

<sup>121</sup> Quintavalla and Temperman.

regulator mengatasi risiko AI secara efisien dan menjaga stabilitas dalam strategi AML yang semakin berbasis AI.

## Kesimpulan

AI berfokus pada pembuatan sistem yang memungkinkan mesin melakukan tugas-tugas kognitif seperti berpikir, komunikasi, dan berperilaku seperti manusia. Salah satu bidang utama AI, *machine learning*, memungkinkan mesin untuk memperoleh pengetahuan dari data secara mandiri. AI telah diaplikasikan di banyak sektor, termasuk keuangan, di mana AI digunakan untuk mendeteksi dan mencegah aktivitas kriminal seperti pencucian uang dengan menganalisis transaksi dan perilaku pelanggan. Di industri perbankan, *machine learning* membantu proses CDD dengan menganalisis data historis dan perilaku pelanggan, memungkinkan bank untuk mengidentifikasi individu berisiko tinggi dan aktivitas mencurigakan dengan lebih efektif. AI juga mengotomatisasi pengambilan keputusan, menghasilkan laporan risiko, memantau transaksi secara terus-menerus, mengurangi biaya kepatuhan, dan meningkatkan respons proaktif terhadap ancaman yang muncul. Teknologi AI dalam e-KYC, peringatan otomatis, dan sistem verifikasi dokumen telah merampingkan prosedur kepatuhan, meningkatkan efisiensi, dan akurasi identifikasi pelanggan, terutama dalam menghadapi meningkatnya risiko dan penipuan perbankan online. Sistem AI juga meningkatkan transparansi dan kepatuhan terhadap peraturan kepemilikan manfaat. Sistem pemantauan transaksi berbasis AI meningkatkan efisiensi dan dapat beradaptasi dengan tren kejahatan keuangan yang muncul.

Namun, AI juga memperkenalkan tantangan etika, termasuk risiko eksploitasi oleh individu yang tidak bertanggung jawab dan berpotensi membahayakan seperti melalui *spear phishing*. Kekhawatiran etis seputar AI dalam layanan keuangan semakin signifikan, terutama dalam kepatuhan AML. Sistem AI dapat membenarkan bias, terutama melalui pembuatan profil berdasarkan etnis atau profesi yang dapat menimbulkan diskriminasi. Privasi adalah masalah utama lainnya, terutama di negara-negara seperti Indonesia yang peraturan privasinya masih berkembang.

Uji proporsionalitas dengan Pasal 28J UUD 1945 memberikan kerangka kerja untuk membatasi hak dengan cara yang menghormati ketertiban umum dan moralitas. Dalam konteks strategi AML berbasis AI, pengujian ini memastikan bahwa hak privasi tidak dilanggar secara berlebihan dan bahwa semua langkah yang diperlukan dan proporsional untuk memerangi aktivitas kriminal sudah dilakukan. Secara praktis, sistem AI harus transparan, efektif, dan tidak invasif. Tantangan dapat muncul, terutama dengan pengawasan aktivitas yang mencurigakan, karena undang-undang AML/CFT saat ini mencegah pemberitahuan individu yang mungkin sedang diselidiki. Amandemen hukum diperlukan untuk meningkatkan transparansi sambil menjaga investigasi dan memastikan bahwa teknologi AI digunakan secara bertanggung jawab dan etis. Undang-undang harus memandu pengembangan AI untuk memastikan keadilan, akuntabilitas, dan transparansi, melindungi hak-hak individu, dan sekaligus menumbuhkan kepercayaan pada teknologi AI.

## Daftar Pustaka

- Ahmed, Faraz. "Ethical Aspects of Artificial Intelligence in Banking." *Journal of Research in Economics and Finance Management* 1, no. 2 (2022): 55–63. <https://doi.org/10.56596/jrefm.v1i2.7>.
- Aluko, Ayodeji and Mahmood Bagheri. "Ethical Aspects of Artificial Intelligence in Banking." *Journal of Money Laundering Control* 15, no. 4 (2012): 442–457. <https://doi.org/10.1108/13685201211266024>.
- Bajgar, Ondrej, and Jan Horenovsky. "Negative Human Rights as a Basis for Long-Term AI Safety and Regulation." *Journal of Artificial Intelligence Research* 76 (2023): 1043–75. <https://doi.org/10.1613/jair.1.14020>.

- Bertrand, Astrid, Winston Maxwell, and Xavier Vamparys. "Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?" *Telecom Paris Research Paper Series* November 2020. <http://dx.doi.org/10.2139/ssrn.3647420>.
- Bieler, S. Alexandra. "Peeking into the House of Cards: Money Laundering, Luxury Real Estate, and the Necessity of Data Verification for the Corporate Transparency Act's Beneficial Ownership Registry." *Fordham Journal of Corporate and Financial Law* 27, no. 85 (2021). <https://heinonline.org/HOL/LandingPage?handle=hein.journals/fjcf27&div=7&id=&page=>.
- Chatterjee, Sheshadri, and Sreenivasulu N.S. "Artificial Intelligence and Human Rights: A Comprehensive Study from Indian Legal and Policy Perspective." *International Journal of Law and Management* 64, no. 1 (2021): 110–34. <https://doi.org/10.1108/ijlma-02-2021-0049>.
- Chitimira, Howard, Elfes Torerai, and Lisa Jana. "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector." *Potchefstroom Electronic Law Journal* 27 (2024). <https://doi.org/10.17159/1727-3781/2024/v27i0a18024>.
- Circumaru, Alexandru. "Towards European AI: Part I - Setting the Context." Qmul.ac.uk, October 18, 2019. <https://www.qmul.ac.uk/euplant/blog/items/towards-european-ai-part-i---setting-the-context-.html>.
- Constitutional Court of the Republic of Indonesia. "Decision Number 14/PUU-VI/2008." Mkri.id, 2020. <https://en.mkri.id/court/decision?search=14%2FPUU-VI%2F2008>.
- Constitutional Court of the Republic of Indonesia. "The 1945 Constitution of the Republic of Indonesia," 2020. <https://en.mkri.id/library/constitution>.
- Conte, Alex. "Limiting Rights under International Law." In *Human Rights in the Prevention and Punishment of Terrorism Commonwealth Approaches: The United Kingdom, Canada, Australia and New Zealand*, 283–314. Springer Nature, 2010. [https://doi.org/10.1007/978-3-642-11608-7\\_10](https://doi.org/10.1007/978-3-642-11608-7_10).
- Dewi, Sinta, and Mohammad Wildan Hidayat. "Protection of Data Privacy in the Era of Artificial Intelligence in the Financial Sector in Indonesia." *Journal of Central Banking Law and Institutions* 1, no. 2 (2022). <https://doi.org/10.21098/jcli.v1i2.18>.
- Digital Finance. "Asia Banks Spend \$45 Billion on Compliance – for What?" Digital Finance, March 13, 2024. <https://www.digfingroup.com/compliance-lexisnexis/>.
- FATF. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," 2023. <https://www.fatf-gafi.org/content/dam/fatf-gafi/Recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>.
- Gupta, Abhishek, Dwijendra Nath Dwivedi, and Jigar Shah. *Artificial Intelligence Applications in Banking and Financial Services. Future of Business and Finance*. Springer, 2023. <https://doi.org/10.1007/978-981-99-2571-1>.
- Gupta, Abhishek, Dwijendra Nath Dwivedi, and Ashish Jain. "Threshold Fine-Tuning of Money Laundering Scenarios through Multi-Dimensional Optimization Techniques." *Journal of Money Laundering Control*, ahead-of-print, no. ahead-of-print (2021). <https://doi.org/10.1108/jmlc-12-2020-0138>.
- Hannan, Md. Abdul, Md. Atik Shahriar, Md. Sadek Ferdous, Mohammad Jabed, and Mohammad Shahriar Rahman. "A Systematic Literature Review of Blockchain-Based E-KYC Systems." *Computing* 105 (2023). <https://doi.org/10.1007/s00607-023-01176-8>.
- Japanese Society for Artificial Intelligence. "The Japanese Society for Artificial Intelligence Ethical Guidelines," 2017. <https://www.ai-gakkai.or.jp/ai-elsi/wp-content/uploads/sites/19/2017/05/JSAI-Ethical-Guidelines-1.pdf>.

- Jullum, Martin, Anders Løland, Ragnar Bang Huseby, Geir Ånonsen, and Johannes Lorentzen. "Detecting Money Laundering Transactions with Machine Learning." *Journal of Money Laundering Control* 23, no. 1 (2020): 173–86. <https://doi.org/10.1108/jmlc-07-2019-0055>.
- Kaur, Guneet. "Trust the Machine and Embrace Artificial Intelligence (AI) to Combat Money Laundering Activities." In *Computational Intelligence for Modern Business Systems Emerging Applications and Strategies*, edited by Sandeep Kautish, Prasenjit Chatterjee, Dragan Pamucar, N. Pradeep, and Deepmala Singh, 63–81. Springer, 2024. [https://doi.org/10.1007/978-981-99-5354-7\\_4](https://doi.org/10.1007/978-981-99-5354-7_4).
- Makmur, Kartini Laras. "Women and Dirty Money: How Women Are Affected By, Involved, and Counter Money Laundering." *Jurnal Hukum Prasada* 9, no. 1 (2022): 35–44. <https://doi.org/10.22225/jhp.9.1.2022.35-44>.
- Makmur, Kartini, and Ahsanul Minan. "Money Laundering/Financing of Terrorism Risks in the Indonesian Islamic Banking System." In *Proceedings of the 3rd International Conference of Islamic Finance and Business*. European Alliance for Innovation, 2023.
- OECD. "AI Principles." OECD, 2024. <https://www.oecd.org/en/topics/sub-issues/ai-principles.html>.
- Prakarsa. "Highlighting Illicit Financial Flow of Indonesia's Top Six Export Commodities." [theparakarsa.org](http://theparakarsa.org), November 2019.
- Press, Gil. "Artificial Intelligence (AI) Defined." *Forbes*, August 28, 2017. <https://www.forbes.com/sites/gilpress/2017/08/27/artificial-intelligence-ai-defined/>.
- Quintavalla, Alberto, and Jeroen Temperman, eds. *Human Rights and Artificial Intelligence*. Oxford University Press, USA, 2023.
- Schlink, Bernhard. "Proportionality in Constitutional Law: Why Everywhere but Here?" *Duke Journal of Comparative & International Law* 22, no. 10 (2012). <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1290&context=djcil>.
- Sieckmann, Jan. "Proportionality as a Universal Human Rights Principle." In *Proportionality in Law*, edited by David Duarte and Jorge Silva Sampaio, 3–24. Springer, 2018. [https://doi.org/10.1007/978-3-319-89647-2\\_1](https://doi.org/10.1007/978-3-319-89647-2_1).
- Śliwiński, Emil. "Principle of Proportionality as a Threat to Criminal-Law-Related Fundamental Rights." *New Journal of European Criminal Law* 14, no. 3 (2023): 203228442311583. <https://doi.org/10.1177/20322844231158323>.
- Sullivan, Morgan. "Big Tech's Evolving Role in AI Governance: Shaping Ethical Standards." *Transcend Blog*, March 21, 2024. <https://transcend.io/blog/big-tech-ai-governance>.
- The European Parliament and The Council. "2016/679 General Data Protection Regulation," 2016.
- The Senate of The United States. "Bill to Provide a Framework for Artificial Intelligence Innovation and Accountability, and for Other Purposes," November 15, 2023. <https://www.congress.gov/118/bills/s3312/BILLS-118s3312is.pdf>.
- UN Human Rights Committee. "General Comment No. 31 [80], the Nature of the General Legal Obligation Imposed on States Parties to the Covenant." *Refworld*, May 26, 2004. <https://www.refworld.org/legal/general/hrc/2004/en/52451>.
- United Nations. "Universal Declaration of Human Rights." United Nations, 1948. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.
- Yeoh, Peter. "Banks' Vulnerabilities to Money Laundering Activities." *Journal of Money Laundering Control* 23, no. 1 (2019): 122–35. <https://doi.org/10.1108/jmlc-05-2019-0040>.