



Artificial intelligence in combating money laundering and terrorist financing in the context of European Union legislation

Sztuczna inteligencja w zwalczaniu prania pieniędzy oraz finansowania terroryzmu w kontekście prawodawstwa Unii Europejskiej

Krzysztof Marian MUCHA

Uniwersytet Opolski

ORCID: 0000-0002-6675-2470

E-mail: krzysztof.mucha@uni.opole.pl

Abstract

The aim of the research conducted as part of this article was to understand the impact of artificial intelligence on the effectiveness of anti-money laundering and counter-terrorism financing measures in the financial sector. The research questions focused on identifying areas where AI can effectively improve preventive measures and on understanding the challenges associated with implementing this technology in the context of financial security. Furthermore, the discussion discussed in this paper analyzed the prospects for the development of artificial intelligence (AI) in anti-money laundering and counter-terrorism financing measures and assessed its impact on the effectiveness of preventive measures. The research hypothesis assumed that developing AI systems could increase the effectiveness of detecting illegal transactions and terrorist activities. The conclusions indicate that AI development is crucial to effectively combating financial crime, but it also requires continuous adaptation to the changing threat environment. The study summary also suggests that investments in AI development in the financial sector are essential to maintaining security and effective financial crime prevention, as well as maintaining financial stability.

Additionally this paper aims to critically examine the digital transformation of anti-money laundering (AML) and countering the financing of terrorism (CFT) in light of the Financial Action Task Force (FATF) San Jose principles, the Organisation for Economic Co-operation and Development (OECD) principles for artificial intelligence (AI) and the recently enacted European Union (EU) Artificial Intelligence Act. Author argues that AI tools can revolutionize AML/CFT and asset recovery, but there is a collateral need to strike a balance between optimizing AML/CFT efficiency and safeguarding fundamental human rights.

Keywords

Artificial intelligence (AI), money laundering, terrorism financing, financial stability, EU law

Streszczenie

Celem przeprowadzonej w ramach niniejszego artykułu analizy było zbadanie wpływu sztucznej inteligencji (AI) na skuteczność działań zapobiegających praniu pieniędzy (ML) oraz finansowaniu terroryzmu (FT) w sektorze finansowym. Podniesione problemy badawcze koncentrowały się na identyfikacji obszarów, w których AI może skutecznie usprawnić działania prewencyjne, jak też na zbadaniu wyzwań związanych z wdrożeniem tej technologii w kontekście bezpieczeństwa finansowego. Ponadto, celem podjętej w pracy dyskusji była analiza perspektyw rozwoju AI w działaniach zapobiegających ML/FT oraz ocena jej wpływu na skuteczność działań prewencyjnych, przy czym hipoteza badawcza zakładała, że rozwijane systemy AI mogą zwiększyć skuteczność wykrywania nielegalnych transakcji i działań terrorystycznych. Konkluzje rozważań wskazują, że rozwój AI ma kluczowe znaczenie dla skutecznej walki z przestępczością finansową, ale jednocześnie wymaga ciągłej adaptacji do zmieniającego się otoczenia zagrożeń, a ponadto aktualizują konieczność inwestycji sektora finansowego, regulatorów i organów rządowych w rozwój AI jako niezbędne dla utrzymania bezpieczeństwa i skutecznego zapobiegania przestępczości finansowej, jak też utrzymania stabilności finansowej.

Jednocześnie niniejszy artykuł ma na celu krytyczną analizę cyfrowej transformacji przeciwdziałania praniu pieniędzy (AML) i finansowaniu terroryzmu (CFT) w świetle tzw. Zasad Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (FATF) z San Jose, Rekomendacji Organizacji Współpracy Gospodarczej i Rozwoju (OECD) dotyczących AI oraz przyjętego na forum Unii Europejskiej (UE) rozporządzenia o sztucznej inteligencji (ang. EU AI Act, rozporządzenie AI). Autor przedstawia linię argumentacyjną wskazującą na to, że narzędzia AI mogą zrewolucjonizować procesy, metodyki i działania AML/CFT, lecz jednocześnie istnieje potrzeba znalezienia równowagi między optymalizacją efektywności AML/CFT a ochroną praw człowieka.

Słowa kluczowe

Sztuczna Inteligencja, pranie pieniędzy, finansowanie terroryzmu, stabilność finansowa, prawo UE

Uwagi ogólne

Mając na uwadze obecną epokę dynamicznego rozwoju technologii, wykorzystanie sztucznej inteligencji (AI)¹ staje się kluczowym narzędziem w różnych dziedzinach, w tym w zwalczaniu przestępczości finansowej, takiej jak pranie pieniędzy (ML) oraz finansowanie terroryzmu (FT).

Celem niniejszego artykułu jest zbadanie roli AI w kontekście wdrażania polityk publicznych i procedur instytucji finansowych służących przeciwdziałaniu praniu pieniędzy (AML) oraz finansowaniu terroryzmu (CFT), w tym analiza potencjalnych korzyści oraz identyfikacja wyzwań związanych z wdrożeniem technologii AI. Problem

¹ Zgodnie z definicją ustanowioną w art. 3 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Akt w sprawie sztucznej inteligencji) (Dz. Urz. UE L, 2024/1689, 12.7.2024) - „system AI” oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne.

badawczy objęty rozważaniami niniejszego artykułu zmierza ku rozstrzygnięciu kwestii, czy wykorzystanie AI może korzystnie wpłynąć na zwalczanie zjawiska ML/FT. Hipoteza badawcza artykułu zakłada, że efektywne wdrożenie AI w systemach AML/CTF instytucji finansowych oraz właściwych organów może znacząco poprawić zdolność wykrywania i ścigania ML/FT, przy czym istotnym założeniem badawczym jest to, że AI, oparta na algorytmach uczenia maszynowego, może skutecznie analizować ogromne ilości danych finansowych, identyfikując wzorce i różnego rodzaju anomalie, które mogą być trudne do wykrycia tradycyjnymi metodami.

Zastosowane w niniejszej analizie metody badawcze obejmują dogłębną analizę literatury naukowej oraz studia przypadków wdrożeń systemów informatycznych w systemach AML/CTF, zaś jednocześnie przedstawione zostaną również innowacyjne podejścia i narzędzia oparte na AI, które mogą mieć rewolucyjny wpływ na zwalczanie ML/FT.

W związku z dynamicznym rozwojem technologii, analiza przedmiotowych zagadnień z perspektywy wykorzystania AI w obszarze bezpieczeństwa finansowego staje się kluczowa dla zrozumienia, jak nowoczesne narzędzia mogą być skutecznie wykorzystywane w walce z przestępczością finansową, przy czym jak podkreśla A.M. Turing – proceder ML/FT stanowi globalne zagrożenie, mające poważny wpływ na stabilność gospodarek i bezpieczeństwo społeczeństw².

Rola AI na rynku usług finansowych

Zanim przeanalizujemy rolę AI w przeciwdziałaniu tym zjawiskom, warto bliżej poznać podstawy teoretyczno-funkcjonalne przedmiotowego procederu. Należy przypomnieć, że ML to proces legalizacji środków uzyskanych nielegalnie, często poprzez ich przekształcenie w pozorne, legalne źródła, zaś często jest to proces wieloetapowy, obejmujący różnorodne transakcje finansowe, mające na celu tzw. zacieranie śladów³.

FT to z kolei dostarczanie środków finansowych lub ich ekwiwalentów na rzecz wspierania działalności terrorystycznej, mogące obejmować finansowanie szkolenia terrorystów, zakupu broni lub finansowania propagandy terrorystycznej, w tym zwłaszcza jest to działalność, której celem jest wspieranie organizacji lub osób zaangażowanych w akty terrorystyczne⁴. Przestępcy stosują różnorodne techniki ML/FT, aby utrudnić ich śledzenie a jedną z najbardziej popularnych jest dzielenie dużych sum pieniędzy na mniejsze transakcje, co ułatwia ich kamuflaż, natomiast inne metody obejmują inwestowanie w nieruchomości, dzieła sztuki lub przedsiębiorstwa, co pozwala na transfer środków do różnych klas aktywów⁵.

² A. M. Turing, *Computing Machinery and Intelligence*, [w:] R. Epstein, G. Roberts, G. Beber (red.), *Parsing the Turing Test. Philosophical and Methodological Issues in the Quest for the Thinking*, Springer Dordrecht 2009, s. 22-37.

³ A. Hanafi, *The Dynamic Aspects of Criminal Act and Criminal Liability in Money Laundering Practices*, "Jurnal Hukum Ius Quia Iustum" 2010, no. 17, s. 54.; por. też A. Hetemi, S. Merovci, O. Gulhan, *Consequences of Money Laundering on Economic Growth -The Case of Kosovo and Its Trade Partners*, "Acta Universitatis Danubius" 2018, no. 14, s. 114

⁴ Ibidem, s.114. .

⁵ Ibidem, s. 114.

Proceder ML/FT generuje szereg negatywnych skutków, w tym na poziomie społecznym prowadzą do zakłóceń konkurencji gospodarczej, wzrostu przestępczości i utraty zaufania do instytucji finansowych. Jednocześnie skutki ekonomiczne obejmują destabilizację systemów finansowych oraz utratę kapitału zarówno poprzez bezpośrednie działania przestępców, jak i ogólny spadek zaufania do danego rynku opanowanego przez piorące pieniądze grupy przestępcze. W kontekście bezpieczeństwa konsekwencje te mogą być katastrofalne, gdyż FT umożliwia grupom terrorystycznym pozyskiwanie funduszy na realizację celów zagrażających porządkowi publicznemu i stabilności społeczeństw, zaś jednocześnie wyprane środki mogą być wykorzystywane do zakupu broni lub przeprowadzania ataków, co zwiększa w opinii N. Hendrijetty i B.S. Grewala ryzyko dla bezpieczeństwa narodowego⁶.

Wskazać trzeba, iż zrozumienie tych podstaw jest kluczem do opracowania skutecznych strategii przeciwdziałania, przy czym analiza mechanizmów ML/FT stanowi niezwykle ważny krok w kierunku opracowania narzędzi, które pozwolą na skuteczną identyfikację, monitorowanie i zwalczanie tych patologii w kontekście globalnej sceny finansowej. W obliczu rosnącego zagrożenia ML/FT, instytucje finansowe na całym świecie poszukują nowoczesnych narzędzi, które pozwolą na skuteczniejsze zwalczanie tego procederu, a AI w tym kontekście wyłania się jako kluczowe narzędzie, które może nie tylko identyfikować schematy ML/FT, ale także – jak trafnie zaznacza P. Stylec-Szromek – dostosowywać się na zasadzie adaptacji oraz samouczenia się do ewoluujących strategii przestępców⁷. Jednocześnie P. Stylec-Szromek podkreśla, że jednym z najważniejszych obszarów, w których AI może zrewolucjonizować walkę z ML/FT, jest analiza bardzo dużych zbiorów danych finansowych, gdyż tradycyjne metody, takie jak audyt finansowy czy badanie oparte na dokumentach często charakteryzują się ograniczoną skalą i złożonością analizowanych danych⁸.

Na tym tle AI, wykorzystując zaawansowane algorytmy uczenia maszynowego, może przetwarzać ogromne ilości informacji, identyfikując subtelne wzorce, które mogą wskazywać na tego typu aktywność. M. Rojszczak zauważa, że w kontekście walki z ML/FT, może być AI wykorzystywana do ciągłego uczenia się na podstawie nowych danych, przy czym algorytmy uczenia maszynowego mogą analizować zachowania finansowe klientów, identyfikując nietypowe transakcje lub podejrzane wzorce⁹. W miarę gromadzenia nowych danych systemy te stają się coraz precyzyjniejsze w rozpoznawaniu nieprawidłowości, na którym to tle można powiedzieć, że systemy te, wraz z nowymi danymi, zyskują coraz więcej możliwości¹⁰.

AI umożliwia automatyczne wykrywanie transakcji, które mogą wskazywać na próby ML/FT, zaś algorytmy mogą oceniać ryzyko związane z daną transakcją na podstawie wielu czynników – takich jak kwota transakcji, lokalizacja, częstotliwość czy

⁶ N. Hendrijetty, B.S. Grewal, *Macroeconomics of Money Laundering: Effects and Measurements*, "Journal of Financial Crime" 2017, no. 24, s. 45.

⁷ P. Stylec-Szromek, *Sztuczna inteligencja – prawo, odpowiedzialność, etyka*, „Organizacja i Zarządzanie” 2018, nr 123, s. 11.

⁸ Ibidem, s. 11.

⁹ M. Rojszczak, *Sztuczna inteligencja w innowacjach finansowych – aspekty prawne i regulacyjne*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2020, nr 2(9), s. 70.

¹⁰ Ibidem, s. 70.

uczestnicy danej transakcji. Tego rodzaju „skanowanie” ekosystemu transakcji finansowych umożliwia to szybką reakcję na potencjalne przypadki udziału w tego typu nielegalnych działaniach¹¹. AI może również odgrywać niezwykle kluczową rolę w analizie zachowań klientów monitorując i analizując interakcje klientów z usługami finansowymi, systemy AI mogą identyfikować nietypowe wzorce, które mogą sugerować próby ML/FT, przy czym podejście to opiera się na zdolności AI do zrozumienia kontekstu transakcji, a także budowania kompleksowego obrazu zachowań finansowych klientów¹².

Wraz z rosnącą popularnością technologii blockchain, AI może być również wykorzystywana do monitorowania transakcji w sieciach opartych na tej technologii, gdyż analizując rejestry rozproszone, AI może identyfikować podejrzane transakcje oraz śledzić przepływ środków w sieci blockchain, co znacznie utrudnia ML/FT. Wskazane uwarunkowania jasno wskazują, że AI staje się kluczowym elementem w walce z ML/FT, a jej zdolność do analizy ogromnych zbiorów danych, ciągłego uczenia się oraz automatycznego wykrywania podejrzanych transakcji sprawia, że jest ona niezbędnym narzędziem dla instytucji finansowych, które dążą do skutecznego przeciwdziałania temu zjawisku¹³.

Inicjatywy FATF – San Jose Principles

Zasady przewodnie San Jose¹⁴, pierwszy zestaw niewiążących zasad (tzw. soft law, miękkie prawo) w tej dziedzinie, zostały sformułowane w 2017 r. przez FATF¹⁵ w kontekście trwającego dialogu między FATF a sektorem prywatnym, w szczególności branżą FinTech. Zasady przewodnie San Jose podkreślają potrzebę ochrony systemu finansowego przed zagrożeniami związanymi z ML/FT (Zasada przewodnia 1) oraz poprzez ramy współpracy i bliską współpracę rządów i sektora prywatnego (Zasada przewodnia 2).

Zasady San Jose zachęcają one również do „pozytywnej i odpowiedzialnej innowacji” (Zasada przewodnia 3) w celu zwiększenia skuteczności systemu AML/CFT w ramach „inteligentnych” ram regulacyjnych (Zasada przewodnia 4), które odnoszą się do ryzyka bez tłumienia innowacji¹⁶. Niemniej jednak wytyczne te są raczej niejasne i nie dostarczają jasności co do szczegółowych cech „odpowiedzialnej innowacji” i „inteligentnych regulacji”. Brakuje w nich również odniesienia do ochrony praw podstawowych, co jest prawdopodobnie najpoważniejszym niedociągnięciem. Zasada przewodnia nr 5 krótko odnosi się do zasad uczciwości, neutralności

¹¹ M. H. Huang, R. T. Rust, Artificial Intelligence in Service, „Journal of Service Research” 2018, no. 21, s. 102-104.

¹² Ibidem, s. 104.

¹³ Ibidem, s. 104.

¹⁴ San Jose Guiding Principles (2017), dostępne pod adresem: www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-fintech-regtech-forum-may-2017.html [dostęp 13.11.2025].

¹⁵ Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF), znana również pod francuską nazwą Groupe d'action financière (GAFI), to organizacja międzyrządowa założona w 1989 roku z inicjatywy G7 w celu opracowywania polityk zwalczania prania pieniędzy i utrzymywania określonych interesów. W 2001 roku jej mandat został rozszerzony o finansowanie terroryzmu. Sekretariat FATF jest administracyjnie zlokalizowany w siedzibie OECD w Paryżu, ale obie organizacje są odrębne.

¹⁶ Por. szerzej G. Pavlidis, Europe in the digital age: regulating digital finance without suffocating innovation, „Law Innovation and Technology” 2021, vol. 13, no. 2, s. 464-477.

handlowej i spójności z międzynarodowym otoczeniem regulacyjnym, przy czym są to jednak oczywiste wartości, które mają zastosowanie do wszystkich ram regulacyjnych, nie tylko do wykorzystania AI w kontekście AML/CFT. Z drugiej strony, Zasady przewodnie z San Jose stanowią – w opinii G. Pavlidisa - pierwszy krok w trwającym procesie konsultacji i należy je postrzegać jako projekt, który może pomóc w ustanowieniu bardziej szczegółowych zasad cyfrowej transformacji AML/CFT¹⁷. Rzeczywiście, ostatnie raporty FATF (FATF, 2021c) są bardziej szczegółowe i podkreślają potrzebę podejścia opartego na ryzyku w celu osiągnięcia wysokiego stopnia wyjaśnialności (ang. explainability) i audytowalności (ang. auditability) oraz ochrony prywatności oraz respektowania innych praw człowieka, jak też stały się podstawą dla opracowania Rekomendacji OECD oraz rozpoczęcia prac nad unijnym rozporządzeniem w sprawie AI¹⁸.

Wytyczne OECD dotyczące AI na tle przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu

W 2019 roku OECD opracowała własny zestaw zasad przewodnich dotyczących promowania AI¹⁹ jako innowacyjnej i godnej zaufania technologii, mającej jednocześnie respektować prawa człowieka i wartości demokratyczne. Zasady OECD traktują AI jako technologię ogólnego przeznaczenia – to znaczy nie w kontekście AML/CFT. Po pierwsze, stwierdzają, że AI powinna promować wzrost sprzyjający włączeniu społecznemu, zrównoważony rozwój i dobrobyt (Zasada 1 OECD), co jest celem ogólnym i niekontrowersyjnym, ale oferuje niewiele szczegółowych wytycznych. Po drugie, stwierdzają, że systemy AI powinny być zgodne z „rządami prawa, prawami człowieka, wartościami demokratycznymi i różnorodnością” (Rekomendacja 2 OECD), z użytecznym odniesieniem do potrzeby „odpowiednich zabezpieczeń, na przykład umożliwiających interwencję człowieka w razie potrzeby”, zaś kluczowym wyzwaniem w tym kontekście jest ustanowienie skutecznych mechanizmów odpowiedniego nadzoru.

Na tle Rekomendacji OECD trzeba wskazać, że odpowiednia regulacja i nadzór wymagają rozwijania wiedzy specjalistycznej w zakresie nowych technologii, zrozumienia ryzyka i umiejętności wdrażania odpowiednich środków ograniczających ryzyko. W związku z tym organy nadzoru AML/CFT powinny być w stanie zdobyć taką wiedzę specjalistyczną, aby skutecznie nadzorować wdrażanie przez podmioty regulowane zabezpieczeń w ich systemach opartych na AI. Rekomendacje OECD wzywają również do większej „przejrzystości i odpowiedzialnego ujawniania informacji dotyczących systemów AI”, aby umożliwić ludziom kwestionowanie wyników (Rekomendacja 3 OECD), co jest ważne, ponieważ decyzje podejmowane przez narzędzia AI nie zawsze są zrozumiałe dla ludzi, których mogą one dotyczyć. Zgodnie z ustanowioną na forum UE zasadą „nieinformowania” w kontekście monitorowania systemu AML/CFT, osoby i podmioty nie są informowane o alertach AML/CFT, które

¹⁷ Ibidem, s. 477.

¹⁸ Ibidem, s. 477.

¹⁹ OECD (2019), Recommendation of the council on artificial intelligence, OECD Recommendation OECD/LEGAL/0449.

ich dotyczą, gdyż tym kontekście przejrzystość nie oznacza informowania osób oznaczonych jako podejrzanane transakcje, ale wymaga, aby metodologia i wyniki modelu AI mogły zostać odpowiednio wyjaśnione i przekazane odpowiednim organom i organom nadzoru nad AML/CFT²⁰. Jest to również związane z pojęciami audytowalności i wyjaśnialności, które wymagają, aby wyniki były powtarzalne przy użyciu tych samych danych wejściowych.

Ponadto Rekomendacje OECD dotyczą kwestii bezpieczeństwa oraz potrzeby ciągłej oceny i zarządzania potencjalnymi zagrożeniami, co oznacza, że „w warunkach normalnego użytkowania, przewidywalnego użytkowania lub niewłaściwego użytkowania bądź innych niekorzystnych warunków, [narzędzia oparte na AI] działają prawidłowo i nie stwarzają nieuzasadnionego ryzyka dla bezpieczeństwa” (Rekomendacja 4 OECD).

W opinii G. Pavlidisa rekomendacja ta jest bardzo podobna do bardziej szczegółowego podejścia UE opartego na ryzyku, przedstawionego w unijnym rozporządzeniu w sprawie AI²¹. Wreszcie, zasady OECD stanowią, że osoby opracowujące, wdrażające lub obsługujące systemy AI powinny ponosić odpowiedzialność za ich prawidłowe funkcjonowanie (Rekomendacja 5 OECD), co w kontekście AML/CFT oznacza, że podmioty regulowane i ich zespoły ds. zgodności odpowiadają za zgodność z przepisami i funkcjonowanie swoich narzędzi opartych na AI. To prowadzi nas do kolejnej ważnej kwestii a mianowicie tego, że narzędzia oparte na AI powinny uzupełniać, a nie zastępować, tradycyjne mechanizmy AML/CFT, takie jak raportowanie transakcji, aby umożliwić zespołom do spraw zapewnienia zgodności skupienie się na analizie, a nie na gromadzeniu i porządkowaniu dużych ilości informacji z różnych źródeł²². Instytucje finansowe nie powinny dążyć do wyeliminowania czynnika ludzkiego w AML/CFT, lecz raczej starać się uwolnić zasoby na przypadki obarczone wyższym ryzykiem, wspierając swoich analityków narzędziami opartymi na AI, nie uchylając się jednak od odpowiedzialności.

Unijne rozporządzenie w sprawie Sztucznej Inteligencji – EU AI Act

W kwietniu 2022 r. Komisja Europejska przedstawiła wniosek dotyczący unijnego aktu prawnego o sztucznej inteligencji (ang. AI Act)²³, który będzie wiążącym instrumentem prawnym na poziomie UE, w przeciwieństwie do wspomnianych wcześniej inicjatyw „miękkiego prawa” FATF i OECD. Inicjatywa UE opiera się na

²⁰ Por. FATF Recommendation No. 21; art. 39 dyrektywy Parlamentu Europejskiego i Rady z 20 maja 2015 r. o przeciwdziałaniu wykorzystywania systemu finansowego do prania pieniędzy i finansowania terroryzmu (wersja ujednolicona Dz. Urz. UE L 141, 5.6.2015, s. 73).

²¹ G. Pavlidis, Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era, „Journal of Money Laundering Control”, 2023, vol. 26, Issue 7, s. 101-106.

²² European Supervisory Authorities (2018), „Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process”, ESA Opinion JC 2017 81.

²³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG) (Dz.U. L, 2024/1689, 12.7.2024).

artykule 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), który stanowi podstawę prawną unijnych instrumentów zapewniających ustanowienie i funkcjonowanie rynku wewnętrznego. W istocie, AI stanowi fundamentalny element jednolitego rynku cyfrowego UE i istnieje potrzeba nowych, zharmonizowanych przepisów dotyczących rozwoju i użytkowania produktów i usług opartych na AI na tym rynku. Wyjaśnia to również wybór rozporządzenia jako instrumentu prawnego, który zapewnia, że nowe przepisy dotyczące AI (definicja, klasyfikacja, zakazy itp.) będą stosowane bezpośrednio i jednolicie, zgodnie z artykułem 288 TFUE. Inicjatywa ma na celu zmniejszenie ryzyka fragmentacji prawnej, ale pozostawia również państwom członkowskim pewną swobodę wyboru sposobu organizacji swoich systemów nadzoru rynku i wdrażania środków promujących innowacje w dziedzinie AI. Proponowany akt jest pierwszą kompleksową inicjatywą ustawodawczą dotyczącą AI, podjętą przez głównego regulatora, mającą na celu zapewnienie przejrzystości i zrozumiałości procesów i wyników, a także nadzoru ze strony człowieka, cyberbezpieczeństwa, ochrony danych i poszanowania prywatności. Od grudnia 2022 r. tekst oczekuje na sfinalizowanie stanowisk Rady Unii Europejskiej i Parlamentu Europejskiego przed negocjacjami międzyinstytucjonalnymi, które obejmują również Preambuła rozporządzenia stanowi, że ustawa o AI nie wpływa na uprawnienia i niezależność organów krajowych i organów nadzorczych w obszarze ochrony danych lub ochrony praw podstawowych. Ponadto poprawki podkreśliły potrzebę wytycznych Komisji Europejskiej dotyczących stosowania przepisów ustawy, w szczególności spójności ich egzekwowania w całej UE, co naszym zdaniem będzie kluczową kwestią na etapie wdrażania, podobnie jak w przypadku większości inicjatyw UE.

Główne przepisy rozporządzenia UE w sprawie AI definiują podejście do AI oparte na ryzyku, w którym ryzyka związane z AI klasyfikuje się następująco:

- ryzyko niedopuszczalne, takie jak punkcja społeczna, które będzie zakazane na mocy ustawy o AI;
- ryzyko wysokie, takie jak wykorzystanie AI w rekrutacji pracowników, wyrobów medycznych itp., które będzie dozwolone pod warunkiem przeprowadzenia przez stronę trzecią oceny *ex ante* zgodności z wymogami dotyczącymi AI, z uwzględnieniem odpowiednich przepisów sektorowych;
- systemy AI o niskim ryzyku, ze szczególnymi obowiązkami w zakresie przejrzystości, takie jak podszywanie się pod człowieka przez tzw. chatboty, które będą dozwolone pod warunkiem powiadomienia ludzi o interakcji z systemem AI;
- oraz aplikacje AI o minimalnym lub zerowym ryzyku, które będą dozwolone bez żadnych ograniczeń²⁴.

To podejście oparte na ryzyku obejmuje staranne rozważenie potencjalnych zagrożeń i negatywnych skutków AI oraz podjęcie kroków w celu ich zapobiegania lub łagodzenia. Przy tym można za poglądem A. Renda argumentować, że podejście oparte na ryzyku do AI może być zbyt ograniczające, podważając tym samym innowacyjność²⁵. Niemniej jednak należy wyrazić opinię, że nie dotyczy to unijnego

²⁴ Por. słowniczek definicji ustanowiony w art. 3 rozporządzenia w sprawie sztucznej inteligencji.

²⁵ A. Renda, *Beyond the brussels effect: leveraging digital regulations for strategic autonomy*, policy brief, strategic autonomy project, foundation for European progressive studies, friedrichebertstiftung, Fondation Jean-Jaurès, Paris 2023.

rozporządzenia o AI, która respektuje zasadę proporcjonalności, ponieważ nakłada obowiązki i obciążenia regulacyjne tylko w przypadkach, w których systemy AI stwarzają wysokie ryzyko²⁶.

W kontekście AML/CFT przepisy unijnego rozporządzenia o AI będą miały również zastosowanie do wykorzystywania AI przez podmioty regulowane i jednostki analityki finansowej (FIU).

Rozporządzenie w sprawie AI i ustanawiana jego normami klasyfikacja ryzyka są zgodne z zasadami FATF San Jose i Rekomendacjami OECD, które opowiadają się za pozytywną i odpowiedzialną innowacyjnością w zakresie AI, uczciwością, przejrzystością i rozliczalnością. Nie jest to zaskakujące, biorąc pod uwagę, że większość państw członkowskich UE jest również członkami FATF i OECD oraz pomaga kształtować pracę i inicjatywy tych organów. Jednakże rozporządzenie UE o AI idzie o krok dalej, ustanawiając szczegółowe obowiązki, zakazy i wyjątki, które mają zastosowanie horyzontalnie do wszystkich systemów AI we wszystkich sektorach, w tym AML/CFT.

Jeśli chodzi o klasyfikację ryzyka, wykorzystanie AI przez podmioty regulowane i jednostki analityki finansowej w kontekście AML/CFT można uznać za wysokiego ryzyka, zgodnie z definicją zawartą w podsekcjach 6(e), (f) i (g) załącznika III do rozporządzenia UE o AI. Rzeczywiście, narzędzia oparte na AI w kontekście AML/CFT celują w osoby w celu zwalczania przestępczości i umożliwiają podmiotom regulowanym, a ostatecznie jednostkom analityki finansowej, przeszukiwanie „złożonych, powiązanych i niepowiązanych dużych zestawów danych dostępnych w różnych źródłach danych lub różnych formatach danych w celu identyfikacji nieznanych wzorców lub odkrycia ukrytych relacji w danych”. Wykorzystanie AI do przeciwdziałania AML/CFT można uznać za część „analizy przestępczości”, ponieważ systemy AML/CFT generują alerty dla niektórych klientów i działań, które mogą być następnie przekazywane do jednostek analityki finansowej (FIU), a następnie do organów ścigania w celu dalszego dochodzenia, postępowania karnego i ostatecznie odzyskania aktywów. W związku z tym kluczowe przepisy unijnej ustawy o AI dotyczące AI wysokiego ryzyka mają również zastosowanie do systemów AI w kontekście AML/CFT.

Ponieważ sektor AML/CFT jest już regulowany, wymogi określone w rozporządzeniu o AI zostaną zintegrowane z istniejącymi procesami i ocenami przeprowadzanymi przez sektorowe organy regulacyjne. Na przykład organy regulacyjne będą musiały zapewnić, że systemy AI wysokiego ryzyka są skutecznie nadzorowane przez osoby fizyczne (art. 14 unijnego rozporządzenia o AI), co oznacza, że powinny one umożliwiać pełną ręczną analizę przez użytkownika w dowolnym momencie (poprzez tzw. przycisk „stop”) i udostępnić uzasadnienie prognoz i decyzji podejmowanych przez AI ludzkiemu nadzorowi (tzw. wyjaśnialność modelu). Zapewni to etyczne i przejrzyste wykorzystanie technologii – na przykład poprzez umożliwienie identyfikacji i korygowania błędów lub uprzedzeń w modelach AML/CFT – budując w ten sposób zaufanie do stosowania AI. Podmioty regulowane i

²⁶ G. Pavlidis, Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era, „Journal of Money Laundering Control” 2023, vol. 26, Issue 7, s. 104.

jednostki analityki finansowej (FIU) korzystające z narzędzi opartych na AI będą musiały również zapewnić zgodność z innymi kluczowymi wymogami ustawy o AI, w szczególności z wysokim poziomem bezpieczeństwa i jakości danych oraz prowadzeniem odpowiedniej dokumentacji, aby umożliwić organom ocenę zgodności. W związku z tym podmioty regulowane i FIU będą musiały opracować nowe struktury zarządzania operacyjnego i ustanowić nowe role, takie jak rola inspektora ds. zgodności z przepisami AI. Z tego powodu okres przejściowy po wejściu w życie unijnego rozporządzenia o AI musi być proporcjonalny do nowego obciążenia związanego z zapewnieniem zgodności nałożonego na twórców i użytkowników narzędzi opartych na AI.

Potencjał wykorzystania AI w przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

W obliczu rosnącego zagrożenia terrorystycznego, skuteczne narzędzia do walki z CFT stają się priorytetem dla instytucji finansowych i organów ścigania. W tym kontekście AI jawi się jako potężne narzędzie, oferując innowacyjne metody analizy i identyfikacji podejrzanych transakcji. Z. Gao i M. Ye już w 2007 r. wskazywali na to, że wdrożenie AI w systemach CFT zapowiada rewolucję w sposobie identyfikacji i eliminacji źródeł finansowania działalności terrorystycznej²⁷.

P. Płoszajski podkreśla, że AI, zwłaszcza w kontekście uczenia maszynowego, pozwala na bardzo dogłębną analizę wielu zmiennych związanych z transakcjami finansowymi, zaś zastosowanie zaawansowanych algorytmów pozwala na identyfikację wzorców, które mogą wskazywać na potencjalne próby finansowania terroryzmu²⁸. Kluczowe jest również monitorowanie nietypowych transakcji, co pozwala na szybkie wykrywanie i reagowanie na potencjalne nieprawidłowości²⁹. Zastosowanie AI umożliwia skuteczniejsze wykrywanie źródeł finansowania terroryzmu. Algorytmy analizują nie tylko same transakcje, ale także powiązania między różnymi podmiotami finansowymi. Dzięki temu możliwa jest identyfikacja wzorców finansowych, które mogą sugerować ukryte kanały transferu środków na cele terrorystyczne. Bowiem tradycyjne metody monitorowania transakcji mogą być niewystarczające w obliczu dynamicznie rozwijających się technik ML/FT. Należy zauważyć, iż AI umożliwia monitorowanie transakcji w czasie rzeczywistym, co zwiększa skuteczność identyfikacji potencjalnie niebezpiecznych operacji.

Pomimo obiecujących perspektyw, wdrażanie AI w walce z finansowaniem terroryzmu nie jest pozbawione wyzwań, a kwestie związane z ochroną prywatności danych, ciągłym doskonaleniem algorytmów i zapewnieniem dostępu do aktualnych danych finansowych stanowią istotne wyzwania w tym obszarze. M. D. Dubber, F. Pasquale, S. Das podkreślają, że konieczne jest również uwzględnienie aspektów

²⁷ Z. Gao, M. Ye, A Framework for Data Mining-Based Anti-Money Laundering Research, "Journal of Money Laundering Control" 2007, no. 10, s.176.

²⁸ P. Płoszajski, Czy nadszedł zmierzch monopolu człowieka na inteligencję? O maszynach myślących jak ludzie i ludziach myślących jak maszyny, Warszawa 2016, s. 17.

²⁹ Ibidem, s.17.

etycznych, aby uniknąć nadużyć i naruszeń praw obywateli³⁰. W dążeniu do skutecznej walki z finansowaniem terroryzmu, AI może być potężnym narzędziem, które może znacząco przyczynić się do zwiększenia skuteczności działań podejmowanych przez instytucje finansowe i organy ścigania, równie ważne, co rozwój technologii, jest jednak także zachowanie równowagi między skutecznością działań a przestrzeganiem praw jednostki i norm etycznych³¹.

Wdrożenie AI w systemach AML/CFT otwiera nowe perspektywy dla instytucji finansowych w zakresie skutecznej identyfikacji i eliminacji nielegalnych działań. Jednym z kluczowych obszarów zastosowania AI w AML/CTF jest analiza zachowań klientów, przy czym algorytmy uczenia maszynowego analizują transakcje klientów, biorąc pod uwagę ich historię, preferencje i charakterystyczne wzorce zachowań a na podstawie tych danych systemy AI mogą identyfikować nietypowe działania, które mogą sugerować próby ML/FT³².

Przykładem może być sytuacja, w której klient, który zazwyczaj dokonuje małych transakcji lokalnych, nagle dokonuje dużej transakcji z krajem objętym sankcjami. System AI, analizując ten kontekst, może automatycznie sklasyfikować transakcję jako podejrzaną i zgłosić ją do dalszej analizy. Analiza Big Data staje się kluczowym narzędziem w walce z ML/FT. Systemy AI, wykorzystując zaawansowane algorytmy przetwarzania danych, mogą analizować ogromne ilości informacji w czasie rzeczywistym. Przykładem praktycznego zastosowania jest monitorowanie transakcji w skali globalnej, a także identyfikacja wzorców wskazujących na potencjalne nieprawidłowości.

AI może być skutecznie wykorzystywana do identyfikacji subtelnych wzorców ML/FT, które mogą wymykać się tradycyjnym metodom analizy. Algorytmy uczenia maszynowego potrafią identyfikować złożone wzorce transakcji charakterystyczne dla ML/FT. Na przykład system AI może wykryć sytuację, w której duże sumy pieniędzy są dzielone na mniejsze transakcje, aby uniknąć podejrzeń³³.

Wdrożenie AI umożliwia również automatyzację procesu zgłaszania podejrzanых transakcji odpowiednim organom ścigania. Algorytmy mogą automatycznie generować raporty w oparciu o ustalone kryteria i przekazywać je organom ścigania. To skutecznie przyspiesza reakcję na potencjalne zagrożenia i usprawnia współpracę z organami regulacyjnymi³⁴. Systemy AI mogą skutecznie identyfikować powiązania między różnymi transakcjami, co jest kluczowe w kontekście AML/CFT. Na przykład, jeśli wiele transakcji wydaje się niepowiązanych, AI może odkryć ukryte powiązania między nimi, sugerujące złożoną działalność przestępczą. Dynamiczny charakter ML/FT wymaga elastycznych systemów, które potrafią dostosowywać się do zmieniających się strategii przestępców. AI, wykorzystując

³⁰ M. D. Dubber, F. Pasquale, S. Das, *The Oxford Handbook of Ethics of AI*, Oxford 2020, s.78.

³¹ T. Hagendorff, *The Ethics of AI Ethics: An Evaluation of Guidelines*, "Minds and Machines" 2020, no. 30, s.115.

³² K. Cyrkun, K. Nastaj-Sałek, R. Sito, H. Noga, W. Jaubiec, *Using artificial intelligence to counter money laundering and terrorist financing*, "ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law" 2024, vol. 28, no. 1, s. 101-106.

³³ M. Rojszczak, *Sztuczna inteligencja w innowacjach finansowych – aspekty prawne i regulacyjne*, "Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2020, no. 2(9), s.75.

³⁴ M.H. Huang, R.T. Rust, *Artificial Intelligence in Service*, "Journal of Service Research" 2018, no. 21, s.167.

uczenie maszynowe, może stale ulepszać swoje algorytmy w oparciu o nowe dane i wykrywać nowe, nieznane wcześniej wzorce.

Wnioski z tych praktycznych przykładów sugerują, że wdrożenie AI w systemach AML/CTF ma potencjał zrewolucjonizowania sposobu, w jaki instytucje finansowe przeciwdziałają ML/FT. Skuteczność AI wynika z jej zdolności do analizowania dużych ilości danych, szybkiego reagowania na nietypowe sytuacje i adaptacji do zmieniającego się otoczenia. Wdrażanie tych technologii staje się zatem kluczowym elementem strategii związanej z AML/CTF.

Perspektywy dalszego rozwoju zastosowań AI w przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

Rozwój AI otwiera nowe perspektywy i stwarza szereg możliwości dla instytucji finansowych i organów regulacyjnych. Poniżej omówimy perspektywy rozwoju AI w kontekście AML/CFT oraz nakreślimy przyszłość, jaka może czekać ten obszar. Perspektywy rozwoju głębokiego uczenia (ang. deep learning) w analizie transakcji są szerokie. Algorytmy oparte na tej technologii mogą doskonale identyfikować nietypowe wzorce, co jest kluczowe w wykrywaniu podejrzanych operacji finansowych. Ewolucja tych algorytmów może prowadzić do powstania jeszcze skuteczniejszych narzędzi do walki z ML/FT³⁵. Rozwój AI umożliwia dalszą automatyzację procesów decyzyjnych w zakresie AML/CFT. Systemy oparte na AI mogą podejmować natychmiastowe decyzje w oparciu o analizę dużych ilości danych, co skraca czas reakcji na potencjalne zagrożenia. Automatyzacja może również zmniejszyć obciążenie pracowników i zwiększyć wydajność operacyjną.

Systemy wykrywania anomalii są kluczowym elementem w AML/CFT. Rozwój AI może prowadzić do powstania bardziej zaawansowanych i dynamicznych narzędzi, które będą w stanie rozpoznawać nawet subtelne zmiany w zachowaniach transakcyjnych. To z kolei pozwoli na skuteczniejszą identyfikację potencjalnych zagrożeń. Perspektywy rozwoju AI obejmują również jej wykorzystanie w zapobieganiu przestępczości finansowej. Algorytmy mogą być wykorzystywane do analizy danych z różnych źródeł, w tym mediów społecznościowych, w celu wczesnego wykrywania potencjalnych działań przestępczych. To proaktywne podejście może zapobiegać nielegalnym działaniom, zanim się rozpoczną.

Perspektywy rozwoju AI w zakresie AML/CTF obejmują również bardziej zaawansowane mechanizmy integracji zbiorów danych na poziomie globalnym. Współpraca między krajami a instytucjami finansowymi może prowadzić do stworzenia bardziej kompleksowych modeli uwzględniających globalne wzorce i trendy. Rozwój AI wymaga jednoczesnego skupienia się na aspektach związanych z cyberbezpieczeństwem. Wraz ze wzrostem roli AI w sektorze finansowym staje się

³⁵ Por. Szerzej: M. Gadre-Patwardhan, S., Katdare, V.V., Joshi, M.R., A Review of Artificially Intelligent Applications in the Financial Domain, [w:] C. Dunis, P. Middleton, A. Karathanasopolous, K. Theofilatos (ed.), Artificial Intelligence in Financial Markets. New Developments in Quantitative Trading and Investment, Palgrave Macmillan, London 2016, s. 76.

ona atrakcyjnym celem dla cyberprzestępców. Ewolucja strategii i technologii bezpieczeństwa jest niezbędna do zachowania integralności systemów³⁶.

Perspektywy rozwoju AI obejmują również poprawę interakcji z użytkownikami. Systemy mogą stać się bardziej intuicyjne, ułatwiając pracę analitykom oraz pracownikom odpowiedzialnym za AML/CTF. Wdrażanie narzędzi ułatwiających interakcję może zwiększyć efektywność działań i ograniczyć liczbę błędów ludzkich. Wraz z postępem technologicznym, AI staje się kluczowym narzędziem w walce z przestępczością finansową. Jednak oprócz korzyści, instytucje muszą skrupulatnie monitorować i dostosowywać swoje systemy, aby sprostać dynamicznym wyzwaniom i zagrożeniom związanym z przyszłym rozwojem tej technologii. Skuteczne wykorzystanie AI w obszarze AML/CTF będzie wymagało elastyczności, innowacyjności i ścisłej współpracy międzysektorowej.

Praktyczne aspekty wdrożenia technologii AI w procesach AML/CTF instytucji finansowych

W tej sekcji omówione zostaną konkretne przykłady zastosowań AI w instytucjach finansowych i organach ścigania, a także narzędzia, technologie i strategie wykorzystywane do analizy danych, identyfikacji wzorców i skutecznego zwalczania działalności przestępczej w dziedzinie finansów i bezpieczeństwa narodowego. Palantir Technologies to amerykańska firma specjalizująca się w analizie danych i AI. Jej platforma, Palantir Gotham, jest szeroko wykorzystywana w sektorach bezpieczeństwa narodowego, AML/CTF. Palantir Gotham umożliwia integrację danych z różnych źródeł, takich jak rządowe bazy danych, informacje z mediów społecznościowych, transakcje finansowe i inne³⁷.

Palantir Gotham wykorzystuje zaawansowane technologie analizy danych, w tym algorytmy uczenia maszynowego, do identyfikacji subtelnych wzorców, które mogą wskazywać na AML/CTF. System umożliwia analitykom dostęp do bogatych zbiorów danych, co pomaga im szybko reagować na potencjalne zagrożenia i podejrzane transakcje. W przypadku zwalczania ML/FT, Palantir Gotham może analizować transakcje finansowe na dużą skalę, identyfikując nieprawidłowości i nieprawidłowości. System umożliwia również śledzenie przepływów finansowych w skali globalnej, co ma kluczowe znaczenie w zwalczaniu ML/FT na poziomie międzynarodowym.

Palantir Technologies współpracuje zarówno z agencjami rządowymi, jak i sektorem prywatnym, dostarczając narzędzia analityczne, które pozwalają na efektywne wykorzystanie potencjału danych w celu przeciwdziałania zagrożeniom związanym ML/FT. Jednak ze względu na specyfikę działań antyterrorystycznych, szczegóły dotyczące konkretnych wdrożeń Palantir Gotham są często traktowane jako poufne.

SAS Institute jest światowym liderem w dziedzinie analityki danych, a ich rozwiązania w zakresie AML są szeroko stosowane w sektorze finansowym. Oparte

³⁶ V. V. L. N. Sastry, *Artificial Intelligence in Financial Services and Banking Industry*, Blue Diamond Publishing, Shabbir 2019, s.11.

³⁷ K. Cyrkun, K. Nastaj-Sałek, R. Sito, H. Noga, W. Jaubiec, op.cit., s. 104.

na AI systemy AML/CFT należące do firmy SAS oferują kompleksowe narzędzia do identyfikacji, monitorowania i zwalczaniu ML/FT. Jednym z kluczowych elementów systemu SAS AML jest wykorzystanie zaawansowanych technologii uczenia maszynowego. Algorytmy te analizują duże ilości danych finansowych, identyfikując nietypowe wzorce transakcji, które mogą wskazywać na nielegalną działalność, przy czym system ten potrafi uczyć się na bieżąco, dostosowując się do zmieniających się strategii przestępczych³⁸.

SAS AML umożliwia bankom i instytucjom finansowym monitorowanie transakcji w czasie rzeczywistym i identyfikację potencjalnych zagrożeń. Analizując dane klientów, system może automatycznie wykrywać podejrzaną transakcję, biorąc pod uwagę różne czynniki, takie jak historia transakcji, profil klienta czy ryzyko związane z określonymi obszarami geograficznymi. Ponadto SAS AML umożliwia automatyczne generowanie raportów zgodności z przepisami prawnymi. System ten jest dostosowany do różnych przepisów i standardów, co pomaga instytucjom finansowym spełniać wymogi prawa dotyczącego AML/CFT. Moduły analityczne umożliwiają również głębszą analizę danych, co wspiera dochodzenia i udział w dochodzeniach prowadzonych przez organy ścigania.

W praktyce instytucje finansowe, takie jak banki i firmy zajmujące się przekazami pieniężnymi, wykorzystują systemy SAS AML do skutecznego podejmowania działań związanych z AML/CFT, jednocześnie wypełniając obowiązki regulacyjne. Z kolei IBM Watson Financial Services to segment IBM oferujący innowacyjne rozwiązania oparte na AI, mające na celu poprawę bezpieczeństwa finansowego oraz AML/CFT. W ramach swoich usług IBM Watson Financial Services oferuje szereg narzędzi i platform analitycznych, które wykorzystują zaawansowane technologie do identyfikacji i monitorowania nielegalnej działalności finansowej³⁹.

Jednym z kluczowych elementów oferty firmy jest platforma IBM Financial Crimes Insights, która integruje dane z różnych źródeł, takich jak transakcje finansowe, informacje o klientach, dane z mediów społecznościowych oraz informacje z otwartych źródeł. Platforma ta wykorzystuje zaawansowane algorytmy uczenia maszynowego, analizując duże ilości danych w czasie rzeczywistym. Z kolei usługa IBM Financial Crimes Insights umożliwia identyfikację nieprawidłowości w zachowaniach transakcyjnych, wykrywanie wzorców związanych z AML/CFT oraz identyfikowanie potencjalnych powiązań z działalnością terrorystyczną, przy czym system ten może automatycznie generować ostrzeżenia i raporty dla analityków finansowych, co przyspiesza reakcję na potencjalne zagrożenia⁴⁰. Ponadto IBM Watson Financial Services oferuje również narzędzia do zarządzania ryzykiem i zgodności z przepisami (RegTech). Systemy te pomagają instytucjom finansowym spełniać rosnące wymagania regulacyjne poprzez automatyzację procesów raportowania, monitorowania i zarządzania ryzykiem. Działania IBM w zakresie finansów i bezpieczeństwa są szeroko wykorzystywane przez instytucje finansowe na całym świecie, a ich innowacyjne podejście do wykorzystania AI wspiera skuteczne działania związane z AML/CFT.

³⁸ Ibidem, s. 104.

³⁹ Ibidem, s. 104.

⁴⁰ Ibidem, s. 104.

Wraz z rozwojem technologii, AI staje się kluczowym narzędziem do AML/CFT. Firmy, instytucje finansowe i organy ścigania na całym świecie wykorzystują zaawansowane algorytmy i systemy AI do analizy danych, identyfikacji wzorców transakcji oraz skutecznego reagowania na potencjalne zagrożenia. Przedstawione przykłady, takie jak systemy SAS Anti-Money Laundering czy platforma Palantir Gotham, pokazują, jak nowoczesne technologie wspierają działania na rzecz bezpieczeństwa finansowego. Integracja AI ze strategiami AML/CFT staje się kluczowym elementem skutecznej ochrony przed dzisiejszymi dynamicznymi zagrożeniami finansowymi i terrorystycznymi⁴¹.

Ograniczenia technologii AI

Wdrażanie AI w przeciwdziałaniu zagrożeniom ML/FT niesie ze sobą szereg wyzwań, którym należy skutecznie sprostać. Pomimo potencjalnych korzyści, jakie AI może przynieść w tych obszarach, istnieją pewne trudności, które mogą wpłynąć na skuteczność tych systemów. Podkreślenia wymaga to, że środowisko AML/CFT jest niezwykle złożone i dynamiczne, zaś przestępcy stale dostosowują swoje taktyki, aby uniknąć wykrycia, co stanowi wyzwanie dla systemów AI. Konieczne jest ciągłe monitorowanie, a także aktualizowanie algorytmów, aby nadążać za nowymi sposobami działania przestępców⁴². Różnorodność schematów AML/CFT utrudnia identyfikację podejrzanych transakcji. Przestępcy stosują różne metody, takie jak dzielenie transakcji na mniejsze kwoty, korzystanie z tzw. „firm śmieciowych” (ang. junk companies) lub wykorzystywanie nowych technologii. AI musi być wystarczająco zaawansowana, aby rozpoznawać te zróżnicowane wzorce i dostosowywać się do nich. Przetwarzanie dużych ilości danych w celu identyfikacji podejrzanych transakcji może prowadzić do naruszenia prywatności klientów. Wdrażając AI, instytucje finansowe muszą znaleźć równowagę między wydajnością operacyjną a poszanowaniem prywatności danych. Konieczne jest zastosowanie odpowiednich mechanizmów ochrony danych i przestrzeganie przepisów dotyczących prywatności. Wprowadzenie AI do istniejących systemów AML/CTF stwarza wyzwania integracyjne. Instytucje finansowe często posiadają złożone i rozbudowane struktury systemowe, które mogą być trudne do modernizacji. Konieczność efektywnego połączenia AI z istniejącymi systemami wymaga starannego planowania i dostosowania do specyfiki danej organizacji. Efektywne wykorzystanie systemów AI wymaga odpowiedniego przeszkolenia personelu, zarówno w zakresie obsługi tych systemów, jak i zrozumienia ich roli w procesie AML/CFT. Edukacja pracowników jest kluczowym elementem sukcesu, pozwalającym uniknąć błędów interpretacyjnych i zmaksymalizować potencjał AI⁴³.

Wprowadzenie AI do systemów finansowych czyni je potencjalnym celem cyberataków. Wymagane są zaawansowane środki bezpieczeństwa, aby chronić systemy AI przed nieautoryzowanym dostępem, atakami hakerów i kradzieżą danych.

⁴¹ Ibidem, s. 104.

⁴² Ibidem, s. 104.

⁴³ V. Dignum, V., Responsible Artificial Intelligence. How to develop and use AI in a responsible way, Dubber 2019, s.58.

W kontekście globalnych rynków finansowych przestępczość transgraniczna stanowi poważne wyzwanie. Systemy AI muszą być zdolne do współpracy i wymiany informacji między różnymi jurysdykcjami, aby skutecznie podejmować działania związane z AML/CFT w skali międzynarodowej.

W obliczu tych wyzwań instytucje finansowe i organy ścigania muszą podchodzić do wdrażania AI z pełnym zrozumieniem i specjalnym przygotowaniem. Działania te wymagają współpracy międzysektorowej, inwestycji w rozwój technologii oraz stałego monitorowania i aktualizacji tych systemów. Wraz z postępem technologicznym, efektywne wykorzystanie AI może przynieść rewolucyjne zmiany w zakresie AML/CFT.⁴⁴

Podsumowanie

Podsumowując problematykę wykorzystania AI w AML/CFT, należy podkreślić znaczący postęp, jaki technologia ta wnosi do sektora finansowego. Celem pracy było zbadanie perspektyw rozwoju AI w kontekście AML/CFT. Celem było również wskazanie nowych możliwości i wyzwań związanych z wdrożeniem tej technologii w procesach związanych z bezpieczeństwem finansowym. Rozwiązanie problemu badawczego polegało na zidentyfikowaniu obszarów, w których AI może skutecznie wspierać instytucje finansowe w zwalczaniu przestępczości finansowej. Przyjęta hipoteza badawcza dotyczyła potencjału wykorzystania AI do usprawnienia systemów AML/CTF oraz zwiększenia skuteczności działań prewencyjnych. Potwierdzeniem hipotezy badawczej jest analiza perspektyw rozwoju AI w zakresie AML/CTF.

Technologia AI staje się niezastąpionym narzędziem w identyfikacji i zwalczaniu nielegalnej działalności finansowej, zaś w szczególności automatyzacja procesów, wykorzystanie głębokiego uczenia (ang. deep learning) i analiza dużych zbiorów danych umożliwiają skuteczniejsze zapobieganie i reagowanie na potencjalne zagrożenia. Wnioski z przedstawionego badania wskazują, że rozwój AI przynosi realne korzyści sektorowi finansowemu w kontekście bezpieczeństwa. Jednak wraz ze wzrostem skuteczności systemów AML/CTF pojawiają się – w opinii M. Anderson oraz L. S. Anderson – nowe wyzwania związane z cyberbezpieczeństwem, etyką stosowania algorytmów oraz koniecznością ciągłego dostosowywania się do zmieniającego się krajobrazu przestępczości finansowej⁴⁵. Artykuł stanowi podstawę do dalszych badań w tej dynamicznie rozwijającej się dziedzinie. Konieczne jest uważne śledzenie postępu technologicznego i dostosowywanie strategii AML/CFT do najnowszych osiągnięć AI. Ostatecznie skuteczność walki z przestępczością finansową będzie zależeć od zdolności instytucji do inteligentnego wykorzystywania i ulepszania narzędzi opartych na AI.

Branża finansowa i informatyczna już rozpoczęła rewolucję w zakresie zgodności z AML/CFT poprzez AI, aby zmniejszyć ryzyko regulacyjne i koszty zgodności oraz zwiększyć efektywność procedur. W istocie trzeba podkreślić to, że wykorzystanie AI w AML/CFT może pomóc w wykrywaniu i zapobieganiu ML/FT poprzez analizę ogromnych ilości danych finansowych i szybką i dokładną

⁴⁴ E. Brynjolfsson, A. Mafee, *Drugi wiek maszyn. Praca, postęp i dobrobyt w czasach genialnych technologii*, Warszawa 2015, s.22.

⁴⁵ M. Anderson, L. S. Anderson, *Machine Ethics: Creating an Ethical Intelligent Agent*, "AI Magazine" 2007, no. 28(4), s.20.

identyfikację podejrzanej aktywności. Jednocześnie jednak – co podnoszą w swoich rozważaniach A. Bertrand, W. Maxwell i X. Vamparys – stwarza nowe wyzwania regulacyjne, w tym prywatność, uczciwość, wyjaśnialność i nadzór⁴⁶.

Zgodność z AML/CFT nie może przekształcić się w dystopijny, masowy nadzór wspomagany przez AI, pozwalający instytucjom finansowym robić to, czego państwa nie mogą zrobić bezpośrednio, zaś z samych tych powodów niezbędne jest ustanowienie zasad i reguł dotyczących AI w AML/CFT, w taki sposób, aby zapewnić odpowiedzialne i etyczne jej stosowanie⁴⁷. Mówiąc dokładniej, należy zapewnić: przejrzystość i rozliczalność, aby osoby opracowujące i wykorzystujące narzędzia oparte na AI mogły ponosić odpowiedzialność za wszelkie negatywne skutki; użytkownicy i nadzorcy mogli zrozumieć, jak działają systemy AI i podejmować decyzje; Systemy AI nie są wykorzystywane do utrwalania dyskryminacji ani uprzedzeń; prywatność i ochrona danych są uwzględniane zgodnie z przepisami i regulacjami dotyczącymi prywatności.

Zasady FATF San Jose i OECD zmierzają w tym kierunku, ale ustawa UE o AI podejmuje bardziej konkretne działania regulacyjne i ustanawia szczegółowe przepisy horyzontalne dotyczące AI, które mają również zastosowanie do AML/CFT. Ostatnim czynnikiem, który należy wziąć pod uwagę, jest potrzeba skoordynowanych działań na szczeblu krajowym i międzynarodowym. Współpraca między właściwymi organami na szczeblu krajowym (FIU, organami ochrony danych i prywatności) jest niezbędna, aby w pełni zrozumieć i ograniczyć ryzyko związane z wykorzystaniem AI w AML/CFT; taka współpraca może mieć charakter zarówno wewnątrzrządowy, jak i publiczno-prywatny. Współpraca międzynarodowa jest niezbędna w celu promowania harmonizacji przepisów, unikania fragmentacji prawnej i zapewnienia, że nowe technologie w zakresie AML/CFT pozostaną zgodne z globalnymi standardami sektorowymi (AML/CFT, prawa człowieka, cyberbezpieczeństwo, prywatność danych itp.).

W tym celu wdrożenie AI do AML/CFT wymaga ciągłego i konstruktywnego dialogu między decydentami, sektorem finansowym i firmami technologicznymi na szczeblu krajowym i międzynarodowym. Tego rodzaju podejście jest nieuniknione, ponieważ, jak słusznie wskazuje P. Yeoh, rola AI w przestępstwach, od cyberataków po przestępstwa finansowe, z dużym prawdopodobieństwem wzrośnie⁴⁸, a wkrótce podmioty regulowane i jednostki analityki finansowej (FIU) będą musiały korzystać z bardziej zaawansowanych narzędzi AI i sprawnego udostępniania informacji, aby przeciwdziałać nowym zagrożeniom. Biorąc to wszystko pod uwagę, decyzja instytucji finansowej lub FIU o inwestycji w narzędzia oparte na AI może przynieść długoterminowe korzyści, jeśli narzędzia te będą wykorzystywane z niezbędną solidnością i spójnością oraz zgodnie z nowymi zasadami zarządzania AI.

Bibliografia

- Anderson M., Anderson L. S., Machine Ethics: Creating an Ethical Intelligent Agent, "AI Magazine" 2007, no. 28(4).
Bertrand A., Maxwell W., Vamparys X., Do AI-based anti-money laundering (AML) systems violate European fundamental rights?, "International Data Privacy Law" 2021, vol. 11, no. 3.

⁴⁶ A. Bertrand, W. Maxwell, X. Vamparys, Do AI-based anti-money laundering (AML) systems violate European fundamental rights?, "International Data Privacy Law" 2021, vol. 11, no. 3, s. 276.

⁴⁷ Ibidem, s. 276.

⁴⁸ Por. szerzej: P. Yeoh, Artificial intelligence: accelerator or panacea for financial crime?, "Journal of Financial Crime" 2019, vol. 26, no. 2, s. 634-646.

- Brynolfsson E., Mafee A., *Drugi wiek maszyn. Praca, postęp i dobrobyt w czasach genialnych technologii*, Warszawa 2015.
- Cyrkun K., Nastaj-Salek K., Sito R., Noga H., Jaubiec W., Using artificial intelligence to counter money laundering and terrorist financing, "ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law" 2024, vol. 28, no. 1.
- Dignum V., *Responsible Artificial Intelligence. How to develop and use AI in a responsible way*, Dubber 2019.
- Dubber M. D., Pasquale F., Das S., *The Oxford Handbook of Ethics of AI*, Oxford 2020.
- Gadre-Patwardhan M., Katdare S., Joshi V.V., A Review of Artificially Intelligent Applications in the Financial Domain, [w:] C. Dunis, P. Middleton, A. Karathanasopolous, K. Theofilatos (ed.), *Artificial Intelligence in Financial Markets. New Developments in Quantitative Trading and Investment*, Palgrave Macmillan, London 2016.
- Gao Z., Ye M., A Framework for Data Mining-Based Anti-Money Laundering Research, "Journal of Money Laundering Control" 2007, no. 10.
- Hagendorff T., The Ethics of AI Ethics: An Evaluation of Guidelines, "Minds and Machines" 2020, no. 30.
- Hanafi A., The Dynamic Aspects of Criminal Act and Criminal Liability in Money Laundering Practices, "Jurnal Hukum Ius Quia Iustum" 2010, no. 17.
- Hendriyetty N., Grewal B.S., Macroeconomics of Money Laundering: Effects and Measurements, "Journal of Financial Crime" 2017, no. 24.
- Hetemi A., Merovci S., Gulhan O., Consequences of Money Laundering on Economic Growth -The Case of Kosovo and Its Trade Partners, "Acta Universitatis Danubius" 2018, no. 14.
- Huang M. H., Rust R. T., Artificial Intelligence in Service, "Journal of Service Research" 2018, no. 21.
- Huang M.H., Rust R.T., Artificial Intelligence in Service, "Journal of Service Research" 2018, no. 21.
- Pavlidis G., Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era, "Journal of Money Laundering Control" 2023, vol. 26, Issue 7.
- Pavlidis G., Europe in the digital age: regulating digital finance without suffocating innovation, "Law Innovation and Technology" 2021, vol. 13, no. 2.
- Płoszajski P., *Czy nadszedł zmierzch monopolu człowieka na inteligencję? O maszynach myślących jak ludzie i ludziach myślących jak maszyny*, Warszawa 2016.
- Renda A., Beyond the brussels effect: leveraging digital regulations for strategic autonomy, policy brief, strategic autonomy project, foundation for European progressive studies, friedrichebertstiftung, Fondation Jean-Jaurès, Paris 2023.
- Rojszczak M., Sztuczna inteligencja w innowacjach finansowych – aspekty prawne i regulacyjne, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2020, nr 2(9).
- Rojszczak M., Sztuczna inteligencja w innowacjach finansowych – aspekty prawne i regulacyjne, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2020, no. 2(9).
- Sastry V. V. L. N., *Artificial Intelligence in Financial Services and Banking Industry*, Blue Diamond Publishing, Shabbir 2019.
- Stylec-Szromek P., Sztuczna inteligencja – prawo, odpowiedzialność, etyka, „Organizacja i Zarządzanie” 2018, nr 123.
- Turing A. M., *Computing Machinery and Intelligence*, [w:] R. Epstein, G. Roberts, G. Beber (red.), *Parsing the Turing Test. Philosophical and Methodological Issues in the Quest for the Thinking*, Springer Dordrecht 2009.
- Yeoh P., Artificial intelligence: accelerator or panacea for financial crime?, "Journal of Financial Crime" 2019, vol. 26, no 2.