Przegląd Bezpieczeństwa Wewnętrznego

2025, nr 33, s. 103–148

 https://doi.org/10.4467/20801335PBW.25.023.22640

ARTYKUŁ

Wykorzystanie analizy behawioralnej w instytucjach obowiązanych w ramach systemu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu

Behaviourist approach as the need to use methods based on recognising customer behaviour in support of the AML/CFT system

MACIEJ ALEKSANDER KĘDZIERSKI

Autor niezależny

https://orcid.org/0000-0003-3074-1355

Abstrakt

Behawiorystyka jako metoda oparta na obserwacji zachowań może być stosowana do profilowania i typowania klientów instytucji obowiązanych jako potencjalnych sprawców i/lub podejrzanych w procederze prania pieniędzy czy finansowania terroryzmu. Dotyczy to zarówno oceny zachowania klienta w bezpośrednim kontakcie z przedstawicielem instytucji, jak i kontaktu klienta z instytucją za pośrednictwem internetu. W pierwszym przypadku istotne jest podejście oparte na psychologii, socjotechnice i retoryce. W drugim wykorzystuje się przede wszystkim najnowsze rozwiązania technologiczne z zastosowaniem sztucznej inteligencji i ślady pozostawiane na urządzeniach mobilnych. Podejście behawioralne do oceny zachowania klienta może być elementem szerszej oceny ryzyka. Podejście to dotyczy relacji klienta z instytucją obowiązaną w ramach wymaganych prawem obowiązków identyfikacji, weryfikacji i monitoringu jego aktywności. Celem artykułu jest potwierdzenie

tezy, że wobec potrzeby analizy ryzyka i typowania środków bezpieczeństwa finansowego w stanie określonego zagrożenia ML/FT wymagane jest od instytucji obowiązanej podjęcie działań w zakresie identyfikacji oraz rozpoznania zachowań klientów z uwzględnieniem czynników behawioralnych.

Słowa kluczowe behawiorystyka, zachowanie, instytucja obowiązana, ryzyko, pranie pieniędzy, finansowanie terroryzmu

Abstract Behavioural science, as a method based on the observation of behaviour, can be widely used to profile and identify clients of obligated institutions as potential perpetrators/suspects in money laundering or terrorist financing. This applies to both the assessment of the client's physical behaviour in the relationship with the institution and their online behaviour, e.g. within the scope of the online banking offer. In the first area, an approach based on psychology, sociotechnics and rhetoric also becomes useful. In the second case, the latest technological solutions based on artificial intelligence and traces left on mobile devices are used. The behavioural approach to the assessment of the client's behaviour, and thus the assessment of the risk associated with it, can be an element of a broader risk assessment. It is part of the client's relationship with the obligated institution as part of the legally required obligations to identify, verify and monitor its activity. The aim of this article is to confirm the thesis that, given the need to analyse risks and select financial security measures in a state of specific ML/FT threat, the obligated institution is required to take action to identify and recognise customer behaviour, taking into account behavioural factors.

Keywords behavioural science, behaviour, obligated institution, risk, money laundering, terrorist financing

Wprowadzenie

Behawioryzm to kierunek w psychologii, który skupia się przede wszystkim na obserwowalnym zachowaniu, a nie na procesach psychicznych, takich jak myślenie i emocje. Zgodnie z tą teorią organizm uczy się przez warunkowanie, które następuje w wyniku interakcji ze środowiskiem, a obserwowalne zachowania są reakcją

na bodźce z zewnątrz. Podejście behawioralne może mieć zastosowanie w różnych dziedzinach nauki, w tym naukach o bezpieczeństwie. Można je wykorzystać m.in. w obszarze przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (ang. Anti-Money Laundering and Countering the Financing of Terrorism, dalej: AML/CFT). W 2000 r. w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (dalej: ustawa o p.p.p.f.t./2000) wprowadzono – jako jedną z zależności przy dokonywaniu analizy w celu określenia wysokości ryzyka w instytucji obowiązanej (dalej: IO) – potrzebę uwzględnienia kryterium behawioralnego, polegającego na nietypowym, w danej sytuacji, zachowaniu klienta (art. 10a ust. 3 pkt 4 ustawy o p.p.p.f.t./2000)[1]. Wprowadzenie tego kryterium wynikało z przekonania, że ta „nietypowość" była czymś spowodowana. Jej przyczyną mogło być to, że organizowanie procederu prania pieniędzy czy finansowania terroryzmu (dalej: ML/FT) mogło mieć wpływ na klienta. Przy czym zachowanie to należy oceniać z dwóch punktów widzenia – jako działanie wyuczone pod wpływem bodźców oraz działanie intuicyjne (zakodowane w umyśle na skutek działań z przeszłości). W wytycznych Europejskiego Urzędu Nadzoru Bankowego (European Banking Authority, EBA)[2] w pkt 2.3. ppkt c wskazano, że: (…) *instytucje powinny uwzględnić ryzyko związane z* (…) *charakterem i zachowaniem klienta i beneficjenta rzeczywistego, w tym instytucje powinny sprawdzić, czy może to wskazywać na zwiększone ryzyko finansowania terroryzmu*. Przy czym zachowanie klienta oznacza w tym przypadku także sposób działania i/lub postępowania, a nie samą reakcję.

W związku z tym, że ryzyko powinno być mierzalne – w celu pozbycia się czynników niepewności (powinny być sprowadzone do poziomu prawdopodobieństwa) i wypracowania środków jego neutralizacji – to zachowanie klienta instytucji również powinno być ujmowane w określone ramy, dzięki którym będzie

[1] *Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*. W *Ustawie z dnia 25 czerwca 2009 r. o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw* w art. 10a ust. 3 pkt 4 wprowadzono nowy zapis, zgodnie z którym: „przy dokonywaniu analizy w celu określenia wysokości ryzyka instytucja obowiązana powinna uwzględnić w szczególności między innymi kryterium: behawioralne – polegające na nietypowym, w danej sytuacji, zachowaniu klienta".

[2] *Wytyczne na podstawie art. 17 i art. 18 ust. 4 dyrektywy (UE) 2015/849 dotyczących środków należytej staranności wobec klienta oraz czynników, które instytucje kredytowe i finansowe powinny uwzględnić podczas oceny ryzyka prania pieniędzy i finansowania terroryzmu związanego z indywidualnymi stosunkami gospodarczymi i transakcjami sporadycznymi („wytyczne w sprawie czynników ryzyka prania pieniędzy i finansowania terroryzmu") uchylające i zastępujące wytyczne JC/2017/37*, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016937/Guidelines%20ML%20TF%20Risk%20Factors_PL.pdf [dostęp: 28 XI 2024].

możliwe jego zmierzenie. Przyjęcie kryterium behawioralnego jako odwołującego się do czegoś mierzalnego jest o tyle istotne, że zachowanie klienta nie powinno być czynnikiem, który zwiększa niepewność (niepewność niemierzalna) i ogranicza możliwość oceny ryzyka stwarzanego przez klienta (prawdopodobieństwo mierzalne). Przyjęcie takiego podejścia wiąże się z opracowaniem indywidualnej skali wartości ryzyka powiązanej z oceną ryzyka instytucjonalnego i operacyjnego IO. Należałoby mieć na uwadze także wzorce działania określonego klienta, takie jak: częstotliwość transakcji, średnia wartość transakcji, typy transakcji i zmiany wzorców transakcji w czasie, wzorce wydatków, lokalizacja transakcji. Te czynniki stwarzają warunki do ujęcia zachowań behawioralnych klienta jako mierzalnych (cechy mogą być przetworzone obiektywnie na algorytm matematyczny, w tym z wykorzystaniem sztucznej inteligencji, ang. *artificial intelligence*, dalej: AI). Jednocześnie wskazuje się na to, że ryzyko jest koncepcją psychologiczną opartą na indywidualnej percepcji, a nie na faktach empirycznych, co może utrudniać ocenę relacji: zachowanie – poziom ryzyka[3]. Z jednej strony zachowanie klienta może być wynikiem określonego rodzaju bodźców związanych z przygotowaniami do czynności kryminalnych i ich podjęciem, a z drugiej specyficzna kumulacja tych bodźców może indywidualnie scharakteryzować jego uzewnętrznione zachowanie. Zastosowanie podejścia behawioralnego w IO wiąże się z oceną zachowania w celu identyfikacji anomalii mogących świadczyć o intensyfikacji ryzyka ML/FT (skali i dynamiki)[4], a także o zachowaniu odzwierciedlającym fazę przestępczego postępowania (planowanie, rozpoznanie, realizacja). Przy takiej ocenie przedstawiciel IO nie uniknie patrzenia na zachowanie klienta z perspektywy kryminologiczno-kryminalistycznej i będzie analizować ryzyko ze względu na potrzebę wprowadzenia adekwatnych środków bezpieczeństwa finansowego. Nie ma to na celu stwierdzenia poczytalności klienta, ale ocenę jego zachowania wobec IO. Z jednej strony takie rozpoznanie IO uwzględnia osobowość przestępcy, jego motywację i postawy życiowe, a z drugiej osobowość potencjalnego sprawcy czynu karnego z punktu widzenia przedmiotu przestępstwa. Umożliwia ustalenie obowiązkowych oznak przestępstwa, takich jak: wiek, poczytalność, nastawienie psychiczne do czynu (w tym przypadku czynników identyfikujących czynności sprawcze ML/FT) itp.[5]

---

[3] P. Slovic, E.U. Weber, *Perception of Risk Posed by Extreme Events*, w: *Regulation of Toxic Substances and Hazardous Waste*, wyd. 2, J.S. Applegate, J.G Laitos, J.M. Gaba, N.M. Sachs (red.), 2011.

[4] Zob. J.R. Meloy i in., *The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology*, „Behavioral Sciences and the Law" 2012, t. 30, nr 3, s. 256–279. https://doi.org/10.1002/bsl.999.

[5] Zob. szerzej: К.А. Викторович, Ш.О. Алексеевна, *Террористический акт: особенности уголовноправовой и криминалистической характеристик*, „Союз Криминалистов

Jako założenie badawcze przyjęto w artykule to, że od IO jest wymagana analiza zachowań klienckich ze względu na potrzebę oceny ryzyka i typowania, a w konsekwencji tej oceny, środków bezpieczeństwa finansowego w stanie określonego zagrożenia ML/FT. Jako cel badawczy wskazano potrzebę rewizji na potrzeby systemu AML/CFT działań związanych z analizą ryzyka opartą na ocenie zachowań klienta.

Celem opracowania jest opis podejścia behawioralnego do analizy ryzyka i rozpoznania zachowania klienta jako podmiotu potencjalnie generującego zachowanie odchyleniowe, które można ocenić negatywnie z punktu widzenia ML/FT. Jako problem badawczy wskazano nie tylko potrzebę pozyskania śladów behawioralnych w celu wstępnej oceny zagrożenia generowanego ze strony klienta IO (dotyczy to początkowych relacji klient – IO i wstępnego typowania ryzyka ze strony klienta), co sugerowałyby zapisy ustawy o p.p.p.f.t./2000, lecz także oceny zachowań klienta w późniejszych relacjach z IO, z wykorzystaniem produktów i usług kwalifikujących jego zachowanie do określonych zachowań nieopartych na wzorcach. Jako metody badawcze wykorzystano analizę tekstu, przegląd literatury oraz ocenę zachowań opartych na korzystaniu z urządzeń identyfikujących relacje klienta z IO w celu pozyskania śladów w systemie AML/CFT, w tym za pośrednictwem biometrii behawioralnej. Podejście behawioralne staje się szczególnym elementem ocennym, gdyż nośnikiem śladów są podmioty fizyczne – klienci, których ocenia się pod kątem ewentualnych zachowań przestępczych.

Kryteria oceny zachowania klienta powinny uwzględniać m.in.: rodzaje transakcji, konta czy rodzaje usług i produktów oferowanych przez instytucje obowiązane. Tym samym IO zostaje zobligowana do opracowania charakterystyki działalności klienta oraz charakteru i celu relacji IO z klientem. W przypadku klienta kojarzonego z FT należy zważyć to, że jeśli postępuje on jako akolita, kibic metod terrorystycznych[6] czy wykonawca, cechuje go zestaw przekonań, które kierują jego zachowaniem i w jego przekonaniu uzasadniają je. Obserwacja zachowań klienta przez IO może pomóc w ujawnieniu pewnych cech, np.: sprzyjania terroryzmowi, skłonności do użycia broni, poglądów ekstremistycznych. Teza rozważań jest

---

и криминологов" (K.A. Wiktorowicz, Sz.O. Aleksiejewna, *Tierroristiczeskij akt: osobiennosti ugołownoprawowoj i kriminalisticzeskoj charaktieristik*, „Sojuz Kriminalistow i Kriminołogow") 2023, nr 1, https://crimeinfo.ru/wp-content/uploads/2023/08/2023-01.pdf, s. 98–104 [dostęp: 28 XI 2024].

[6] Zob. J.P. Bjelopera, *The Islamic State's Acolytes and the Challenges They Pose to U.S. Law Enforcement*, https://sgp.fas.org/crs/terror/R44110.pdf [dostęp: 29 X 2025]; N.M.H. Al-Obaidi, *Motives of the Terrorism Phenomenon Among Youth and the Role of Laws in Dealing with It*, „Akkad Journal of Law and Public Policy" 2021, nr 4, t. 1, s. 182–197. https://doi.org/10.55202/ajlpp.v1i4.85. Na potrzeby artykułu autor przyjął, że „akolita" to zwolennik terroryzmu, chcący na jakimś etapie zaangażować się w działania terrorystyczne jako czynny uczestnik. Natomiast „kibic metod terrorystycznych" to osoba wspierająca metody terrorystyczne z dystansu, np. przez finansowanie, publiczne ich popieranie, m.in. w mediach społecznościowych, a także chcąca pozostać w jakimś zakresie anonimowa.

następująca – w ocenie ryzyka IO powinna uwzględniać zarówno czynniki psychologiczne, jak i obserwowalne zachowania klienta. Tylko takie podejście umożliwia kompleksową ocenę klienta typowanego jako potencjalny sprawca przestępstw ML/FT. Pojawia się pytanie, na ile IO jest w stanie właściwie ocenić zachowanie klienta, czy jest ono skutkiem oddziaływania bodźca zewnętrznego, czy wyrazem funkcjonowania jego psychiki.

Wykorzystanie analizy behawioralnej w IO w kontekście oceny ryzyka ML/FT

Analiza behawioralna pozwala pracownikom instytucji finansowych na wykrywanie nietypowych wzorców zachowań i anomalii w transakcjach klientów związanych zarówno ze świadomym wykorzystaniem produktów i/lub usług na potrzeby przestępcze, jak i tworzeniem nietypowych sposobów posługiwania się produktami i/lub usługami[7] zaoferowanymi przez IO (jako efekt uogólnionej analizy) oraz ocenę ryzyka związanego z działaniami konkretnego klienta. Środki należytej staranności stosowane wobec klienta obejmujące ocenę klientów i zrozumienie ich zachowań odgrywają kluczową rolę w zwalczaniu ML/FT. Ponadto podejście behawioralne, zwłaszcza to oparte na weryfikacji zachowania klienta, pozostaje zbieżne z identyfikacją i weryfikacją klienta indywidualnego w procesie AML/CFT, a także przy określaniu innych zachowań sprawczych dotyczących przestępstw pierwotnych dla ML i FT (np. oszustw). Identyfikacja i weryfikacja klienta są oparte na indywidualizacji zachowań oraz mogą posłużyć do personalizowania produktów i/lub usług, a w konsekwencji do nadania klientowi cech wyjątkowych, które będą go wyróżniały spośród innych klientów (ten zakres nie dotyczy zachowań przestępczych). W tym zakresie IO może skorzystać ze wsparcia AI. Modele AI potrafią pozyskiwać wzorce i zachowania reprezentowane w danych transakcyjnych i interakcjach z klientami i uczyć się ich, a także przetwarzać inne istotne dane. Do profilowania sprawcy ML/FT można wykorzystać wnioski z profilowania marketingowego klientów. W tym zakresie ocena zachowania ma na celu określenie stopnia zaangażowania klienta w proceder przestępczy i czynników, które się do tego przyczyniły. Na analizę behawioralną w kontekście AML/CFT należałoby spojrzeć jako na ocenę zachowania, które powinno się wydawać nienaturalne w danych okolicznościach i kojarzyć się z ML/FT, a więc zachowania klasyfikowanego przez IO jako podejrzane.

[7] Za „typowy" wzorzec zostanie przyjęty sposób postępowania z produktem i/lub usługą, jaki został ustalony w IO przed wprowadzeniem ich na rynek. Wzorzec ten obejmuje posługiwanie się nimi w granicach prawa (np. ustaw i wewnętrznych przepisów w IO).

Podejrzane zachowanie odnosi się do transakcji lub wzorców aktywności, które są nietypowe lub niezgodne ze znanym zachowaniem lub profilem klienta (np. zmiany rodzajów transakcji, beneficjentów lub metod postępowania bez wyraźnego uzasadnienia, odbiegające od regularnych wzorców). Na potrzeby podejmowania wskazanych działań oceny ryzyka w IO jest niezbędne wprowadzenie analityki behawioralnej[8]. Instytucja obowiązana powinna zdefiniować naturalny wzorzec zachowania zindywidualizowanego klienta (profil normalnego zachowania)[9], aby można było porównać go z przedmiotowym wzorcem. Wynik wskazujący na podejrzane zachowanie sygnalizowałby potencjalne ryzyko, a w konsekwencji potrzebę zastosowania środków bezpieczeństwa finansowego. Analityka behawioralna odpowiada za analizowanie interakcji klientów, rozróżnienie wzorca, a ostatecznie profilu oczekiwanego zachowania. Można zbadać, jakie bodźce działały na klienta, który pod ich wpływem nie realizuje wzorca opartego na oferowanym produkcie finansowym. Istnieje wiele możliwości wykorzystania na rzecz analizy behawioralnej i wykrywania anomalii metod opartych na uczeniu maszynowym. Pomagają one identyfikować wzorce przestępstw finansowych przez tworzenie alertów na poziomie triażu na podstawie poziomów ryzyka, dynamicznej oceny ryzyka klienta. Ocena ta łączy zachowania transakcyjne z weryfikacją danych zewnętrznych i istniejącymi alertami opartymi na regułach w celu obliczenia indywidualnego wyniku ryzyka, a także analizy sieci wykorzystującej duże ilości danych o płatnościach do identyfikacji klastrów powiązanych kont w bazie klientów dostawców usług płatniczych[10].

---

[8] Analityka behawioralna to dziedzina zajmująca się gromadzeniem, pomiarem i analizą danych użytkowników z kanałów cyfrowych (takich jak strony internetowe, aplikacje i inne platformy online), aby zrozumieć, w jaki sposób ludzie wchodzą w interakcje i zachowują się, a ostatecznie dlaczego to robią. Celem tej analizy jest odkrycie wzorców, trendów dotyczących motywacji, preferencji i zachowań użytkowników, co umożliwia organizacjom podejmowanie świadomych decyzji, ulepszanie doświadczeń użytkowników, optymalizację strategii i personalizację ofert. Zob. E. Estevez, *Behavioral Analytics: Meaning, Types, Criticism*, Investopedia, 29 I 2023 r., https://www.investopedia.com/terms/b/behavioral-analytics.asp [dostęp: 15 VII 2025]. W omawianym przypadku ocenę zachowań należałoby oprzeć na zdecydowanie szerszym polu ocennym niż tylko tych, do których odnoszą się kanały cyfrowe. Ma to związek także z konwencjonalnymi metodami realizacji produktów i usług finansowych z IO.

[9] Profil normalny może być efektem przyjęcia w IO standardowego postępowania z produktem oraz dotychczasowego funkcjonowania klienta w relacji klient – IO, która zostanie przez IO przyjęta pozytywnie. Tym samym profil normalny będzie wynikiem wypadkowej ogólnego standardu oraz szczególnej pozytywnej oceny indywidualnego zachowania.

[10] R. Francis, L. He, *Managing money laundering risks in digital payments. How digital payment providers can combat financial crime*, OliverWyman, https://www.oliverwyman.com/our-expertise/insights/2023/oct/anti-money-laundering-strategies-for-digital-payment-providers.html [dostęp: 15 VII 2025].

Początkowo behawiorystykę kojarzono wyłącznie z obserwacją fizycznego zachowania klienta w IO. Współcześnie podchodzi się do niej szerzej, np. wykorzystuje się w biometrii, służącej do identyfikacji i weryfikacji klienta po jego unikalne cechy biometryczne. Zmieniło się również spojrzenie na pierwotną ideę behawioryzmu i aktualnie dominuje nurt poznawczo-behawioralny. Ta poznawczość w zakresie AML/CFT oznacza łączenie umiejętności obserwacji przez decydenta IO ze zrozumieniem zachowań klientów i aktualną wiedzą na temat taktyk ML/FT. Wsparciem będzie użycie kryterium behawioralnego pozwalającego poznać wiedzę klienta o usłudze, sposobie korzystania z niej oraz reakcje i postawy klienta w zakresie propozycji komercyjnych (np. w zakresie budowania kapitału, pomnażania zysków, dywersyfikacji inwestycyjnej, lokowania środków finansowych). Pomocniczym instrumentem może okazać się analiza wzorców transakcji dokonywanych przez konkretnego klienta. Pozyskany materiał pozwala na sklasyfikowanie nietypowych zachowań, np. nieregularności czasowej czy kwotowej. W ocenie behawioralnej klienta w bankowości zarówno tradycyjnej, jak i internetowej istotne są takie czynniki, jak m.in.: rozwód, śmierć w rodzinie, utrata pracy, brak mobilności społecznej, uwarunkowania etniczne, rytualne (odnoszenie się do symboli, mistycyzmu, powtarzalnych zachowań) czy doświadczenie dyskryminacji. Podejście behawioralne dotyczy też ocen budowanych na podstawie obserwacji mechanizmu: „bodziec – reakcja" oraz „wzmocnienie – kara". W pierwszym przypadku następuje zawężenie obserwacji i oceny jedynie do zachowania klienta jako podmiotu ocenianego z punktu widzenia procedury „Poznaj swojego klienta" (ang. Know Your Customer, KYC). Takie podejście jest niewystarczające. Ocenę należałoby poszerzyć o kwestie związane z obserwacją zachowania klienta przy założeniu, że może on działać pod wpływem wcześniejszego bodźca (np. wyuczonego na potrzeby realizacji przygotowania do przestępstwa). Te bodźce mogą być niezależne od klienta, np. jako efekt naśladownictwa zauważonych sytuacji kojarzonych z ML/FT, albo zależne, np. jako działanie w wyniku stymulacji podmiotu zewnętrznego (organizatora przestępczego procederu)[11]. Taką typową relacją może być relacja tzw. słup – organizator i/lub inspirator procederu przestępczego (dla ML) czy relacja klient – mentor, charyzmatyczny przywódca (dla FT). W tym drugim przypadku jest możliwe prowadzenie oceny zachowania klienta, gdy wzmocnienie bodźców behawioralnych przychodzi ze strony np. doradcy sprzedażowego w banku. Możliwe jest także obserwowanie reakcji klienta, któremu zależy na pozytywnym zrealizowaniu przedstawionej propozycji bądź będzie chciał się z niej wycofać z uwagi na jej nieadekwatność do przyjętego przez niego wzorca działania przestępczego (np. w wyniku zwiększenia

[11] Tego typu zachowania były zauważane przez pracowników banków, dotyczyły zakładania kont na tzw. słupy na potrzeby karuzel podatkowych.

się możliwości uzyskania śladów aktywności, braku pewności co do realizacji celu przestępczego, wystąpienia obaw związanych z niezrealizowaniem przedsięwzięcia przestępczego i negatywną reakcją jego inicjatora). W ramach analizy ryzyka ML/FT podejście behawioralne można zatem wykorzystać do oceny ryzyka związanego z:

– zachowaniem klienta, zwłaszcza w relacji z IO[12],
– zachowaniami transakcyjnymi klienta[13].

Klientowi mogą towarzyszyć różnego rodzaju emocje i stany psychiczne, jak: lęk, obawy, zdenerwowanie. Stąd też z perspektywy behawioralnej liniowe[14], statyczne podejście do oceny zachowania klienta może być niewystarczające. Warto uzupełnić je podejściem dynamicznym, w ramach którego poszukuje się determinant i bodźców zmiennych w czasie, aby wpłynąć na zmienność zachowania klienta i obserwować jego zachowanie w czasie, a tym samym ujawnić rzeczywiste motywacje[15]. Ryzyko angażowania się klienta w ML/FT stanowi sumę czynników związanych nie tylko z nim jako jednostką, lecz także z sytuacją, otoczeniem i potencjalnym celem przestępczym. Podejście dynamiczne w ocenie zachowania klienta będzie ponadto związane ze zmianami na rynku finansowym, na którym działa większość IO. Jest możliwe również zapewnienie dynamicznej oceny zachowania klienta bez ingerencji ze strony IO. Obserwację mechanizmu „bodziec – reakcja" można wykorzystać zarówno w bezpośrednim kontakcie klienta z przedstawicielem IO, jak i w kontakcie

[12] Przedstawiciel banku powinien wziąć pod uwagę czynniki behawioralne, które mogą wskazywać, że klient np. jest pod wpływem środków odurzających, nie działa samodzielnie, nie jest świadomy, że nawiązuje relacje z bankiem (nie ma świadomości, że podjęte działania oznaczają zawarcie umowy, np. na prowadzenie rachunku). Zob. *Stanowisko Urzędu Komisji Nadzoru Finansowego dotyczące identyfikacji klienta instytucjonalnego i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideoweryfikacji*, https://static.fintek.pl/uploads/2022/03/Stanowisko_UKNF_dot_wideoweryfikacji_klientow_instytucjonalnych.pdf, s. 5 [dostęp: 28 XI 2024].

[13] Ten zakres może dotyczyć np. częstotliwości dokonywania zleceń transakcji, ich złożoności, zachowania klienta przy problemach z czasem ich realizacji, brakiem otrzymania środków przez beneficjenta zlecenia, korzystania z określonych wzorców transakcyjnych – typowanych jako wzorce wysokiego ryzyka itp.

[14] Zob. *Comparison: Terrorist Financing, Money Laundering, and Financing the Proliferation of Weapons of Mass Destruction*, Jersey Financial Services Commission, 14 IV 2022 r., https://www.jerseyfsc.org/industry/guidance-and-policy/comparison-terrorist-financing-money-laundering-and-financing-the-proliferation-of-weapons-of-mass-destruction/ [dostęp: 12 X 2025]; *Counter Proliferation Financing. Guidance Notes*, https://www.fsc.gi/uploads/CPF%20Guidance%20Notes.pdf [dostęp: 12 X 2025].

[15] Dla przykładu, niezmienność w zachowaniach klienta może świadczyć o tym, że zarządza on kontem uśpionym, a zmienność, że pozostaje bezpośrednio powiązany z zarządzaniem aktywami mającymi służyć przygotowaniu aktu terrorystycznego.

online. Możliwe jest także celowe stymulowanie dyskrecjonalne, jeżeli monitoring klienta będzie realizowany bez jego wiedzy (na takie podejście pozwalają ocena ryzyka i środki bezpieczeństwa finansowego podejmowane w ramach AML/CFT). Przedmiotowe podejście jest skuteczniejsze w przypadku biernej postawy klienta, a niepotrzebne w sytuacji, gdy wykazuje on inicjatywę w działaniu. Należałoby także zwrócić uwagę na klientów prowadzących działalność, w której nie popełniają przestępstw pierwotnych, ale piorą pieniądze z innych przestępstw w ramach swojej w innym przypadku legalnej działalności. Obserwowane zachowanie klienta może być wyrazem chęci zaspokojenia potrzeby bezpieczeństwa. Bodźcem może być upadający biznes, groźba bezrobocia, a nawet zagrożenie fizyczne (szantaż, kierowane groźby, zagrożenie dla innych członków rodziny)[16]. Ocena psychologiczna ze strony IO powinna być prowadzona wobec takiego klienta, który jednocześnie może być sprawcą i ofiarą, aby pozyskać wiedzę na temat rzeczywistych powodów podejrzanego zachowania oraz realnego inicjatora. Tego typu zachowanie może być uzewnętrznione jako desperackie, gdy klient działa pod wpływem zdenerwowania, braku realnej oceny zagrożenia, chęci zachowania pozytywnych relacji z IO. Klient może prezentować zaskakujące zachowania w ocenie IO, dokonywać niepotrzebnych zmian aktualnego profilu biznesowego, podejmować nieracjonalne decyzje, zrezygnować z usług, które mogą kojarzyć się z nadmiernym nadzorem ze strony instytucji.

Podejście behawioralne może być także podstawą do odróżniania klienta „zwykłego" i „przestępczego". W tym zakresie istotne jest przyglądanie się zachowaniom marketingowym klienta w IO. Klienci „zwykli" wybierają najchętniej takie produkty lub usługi, które maksymalizują otrzymywaną przez nich wartość. Wartość dla klienta bywa definiowana jako suma użyteczności oferowana nabywcy. Wartość dostarczona klientowi jest różnicą pomiędzy całkowitą wartością produktu dla klienta a kosztem, jaki musi on ponieść w związku z jego pozyskaniem. Jest to więc stan określonej kalkulacji finansowej[17]. U klienta „przestępczego" taki koszt został wliczony w cenę popełnionego przestępstwa pierwotnego. Niejednokrotnie przestępstwo ML jest dokonywane z jakąś stratą aktywów, aby było możliwe zalegalizowanie ich pozostałej części, także tej uzyskanej nielegalnie. To jest

[16] D. Thomas, *Profiling Part 1: The Psychology of Anti Money Launderers*, https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/governance-risk-compliance/white-paper/the-psychology-of-money-launderers.pdf [dostęp: 28 XI 2024].

[17] R. Wolniak, B. Skotnicka-Zasadzień, *Wybrane metody badania satysfakcji klienta i oceny dostawców w organizacjach*, https://www.researchgate.net/profile/Radoslaw-Wolniak/publication/41199963_Wybrane_metody_badania_satysfakcji_klienta_i_oceny_dostawcow_w_organizacjach/links/5ab63b2ba6fdcc46d3b45829/Wybrane-metody-badania-satysfakcji-klienta-i-oceny-dostawcow-w-organizacjach.pdf, s. 31 [dostęp: 18 XI 2024].

przede wszystkim koszt zaangażowania środków zarówno w celu ich odzyskania z pozyskanych aktywów, jak i pomnożenia. Zyskiem w tym przypadku jest status legalności środków, które ponownie będzie można zainwestować (koszty operacyjne zysku przestępczego). W takiej sytuacji kryterium ceny zostaje przesunięte poza IO (zwłaszcza gdy IO ma charakter komercyjny). Istotne staje się natomiast kryterium funkcjonalności produktu i/lub usługi, co należałoby wiązać z cechami bezpośredniej eksploatacji produktu. Tę ocenę można łączyć z dysfunkcjonalnością czasową generowania zysków z aktywów klienta, widocznych dla IO. Funkcjonalność należałoby postrzegać jako ocenę klienta jako sprawcy do posłużenia się takim, a nie innym produktem i/lub usługą w celu realizacji zamierzonego celu przestępczego. Zachowanie się klienta jako sprawcy staje się także konfiguracją działań pozaekonomicznych, które mogą być sklasyfikowane w pozainstytucjonalnej przestrzeni ekonomiczno-administracyjnej (dotyczy to np. zachowań konsumpcyjnych)[18]. Określone zachowanie klienta może być związane z decyzją o przeprowadzeniu zamachu terrorystycznego (np. pilne wystąpienie o rozwiązanie umowy o prowadzenie konta, przekazanie środków członkom rodziny, zlecenie przekazu środków na rzecz radykalnej organizacji, utrudniony kontakt IO – klient). Obserwacja i ocena zachowania klienta pozwalają także uzyskać wiedzę na temat nie tylko jego wyjściowej postawy, lecz także radykalizacji poglądów mogącej prowadzić do rozwiązań siłowych jako behawioralnych skutków radykalizacji. Stąd przedmiotem rozpatrywania może być również przejście od radykalizacji poznawczej do radykalizacji behawioralnej. Należy mieć to na uwadze przy finansowaniu terroryzmu oraz organizacji samych przestępstw terrorystycznych. Zmiana zachowań klienta w relacji z IO może być skutkiem zmian, które zaszły w jego osobowości pod wpływem radykalnych idei[19].

---

[18] *Major factors influencing consumer behavior*, Clootrack, https://www.clootrack.com/knowledge-base/major-factors-influencing-consumer-behavior [dostęp: 18 XI 2024]. Na decyzje zakupowe wpływają np. wiek, dochody i zawód kupującego, jego podejście do określonych produktów lub usług, media społecznościowe, normy kulturowe, tradycje i wartości.

[19] Komisja Europejska wskazuje czynniki mające wpływ na radykalizację. Są to m.in.: czynniki indywidualne (np. poczucie alienacji, niesprawiedliwości, bycia ofiarą), czynniki społeczne (wykluczenie społeczne, faktyczna lub postrzegana dyskryminacja, ograniczona mobilność społeczna), czynniki polityczne (poglądy na temat skutków działań politycznych, wydarzeń i konfliktów), czynniki ideologiczne i religijne, czynniki kulturowe (marginalizacja kulturowa, solidarność z daną grupą etniczną/religijną), działania radykałów i osób zajmujących się rekrutacją m.in. do grup terrorystycznych czy ekstremistycznych, wpływ mediów społecznościowych. Zob. M. Ranstrop, *The Root Causes of Violent Extremism*, Brussels: European Commission, 2016, w: J. Mazurczak, *Radykalizacja jako proces prowadzący do ekstremizmu i terroryzmu*, „Miscellanea Anthropologica et Sociologica" 2020, nr 21(2), s. 45–73.

Do typowania zachowań klienta jako niewłaściwych można przyjąć jako wyróżnik czynnik temporalny (czasowy). Dla przykładu może wystąpić dysfunkcja czasowa kosztów i zysków obserwowalnych aktywów lub dysfunkcja czasowa aktywności klienta w przeszłości i obecnej. Ponadto jest możliwe wnioskowanie o nietypowym zachowaniu na podstawie dysfunkcji czasowej dokonywanych zleceń transakcji, gdy nie ma logicznego wyjaśnienia ich istoty. Kolejnym czynnikiem kształtującym zachowanie klienta jako sprawcy może być wiedza ekonomiczno-finansowa, która wyróżnia zwłaszcza sprawców przestępstw gospodarczych zbliżonych do przestępstw ML/FT. Wiedza ekonomiczno-finansowa pozwala sprawcom na jej wykorzystanie w zakresie teoretycznym lub praktycznym do organizacji przestępstw. Zwłaszcza w IO z sektora finansowego i gospodarczego będzie można zauważyć i ocenić stopień umiejętności i profesjonalizmu przy dokonywaniu przestępstw ML/FT. Sprawcy przestępstw ekonomiczno-finansowych różnią się od sprawców innego rodzaju przestępstw ze względu na istnienie pewnych właściwości. Znają przepisy, które regulują obszar ich pracy zawodowej, i wykorzystują pewne luki prawne, niejasności oraz częste zmiany przepisów, aby działać na granicy prawa[20].

Nie jest także wykluczone, aby pracownik IO przeprowadził z klientem wywiad behawioralny, który – zbliżony do oceny psychologicznej – pozwoliłby decydentowi w IO podjąć decyzję co do dalszego postępowania w rozpoznaniu ryzyka. Ta sytuacja będzie mogła dotyczyć zarówno akolity (kibica) terrorystycznego, jak i samoorganizującego się terrorysty (np. samotnego wilka lub naśladowcy). Tu pomocne będzie zarówno podejście oparte np. na teorii uczenia się zachowań[21], jak i teorii poznawczej (ang. *cognitive theories*). Celem takiego wywiadu byłoby ustalenie korelatów obserwowanego zachowania w relacji klient – IO, a nie formułowanie oceny w ramach koincydencyjnego podejścia. Zastosowany wywiad behawioralny w zakresie KYC miałby na celu zidentyfikowanie takich czynników, jak: indywidualne czynniki społeczno-psychologiczne, czynniki społeczne, kulturowe, a przy korzystaniu przez IO z otwartych źródeł informacji także ocenę wpływu mediów społecznościowych[22].

[20] K. Milanovic, *Money Laundering and Other Forms of Financial Crime*, „Journal of Law and Politics" 2024, nr 5, s. 57–78. https://doi.org//10.69648/JJDU2862.

[21] Na przykład teoria społeczno-poznawcza Alberta Bandury. Zob. A. Bandura, *Teoria społecznego uczenia się*, Warszawa 2007.

[22] Zob. szerzej: J. Mazurczak, *Radykalizacja jako proces prowadzący do ekstremizmu i terroryzmu*, „Miscellanea Anthropologica et Sociologica" 2020, nr 21(2), s. 45–73.

Wymogi związane z podejściem behawioralnym w ramach AML/CFT

Aktualne przepisy ustawy z 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[23] (dalej: ustawa o p.p.p.f.t./2018) nie wskazują wprost potrzeby uwzględniania zachowań klienta w ocenie czynników ryzyka. Niemniej jednak pośrednio wskazują na to zapisy tej ustawy odnoszące się do gradacji stosowania środków bezpieczeństwa finansowego. Instytucje obowiązane powinny budować profile behawioralne swoich klientów na potrzeby oceny ryzyka i stosowania środków bezpieczeństwa finansowego. Przy czym podejście IO powinno koncentrować się zwłaszcza na analizie behawioralnej (w tym przypadku przyjmijmy oceny zachowania zewnętrznego klienta będącego efektem zarówno impulsu wewnętrznego, jak i zewnętrznego wobec niego samego), a nie wyłącznie na analizie zachowań klienta (w którym jako jedyny przedmiot oceny uznaje się jego uzewnętrznione zachowanie jako efekt impulsu zewnętrznego wzbudzającego emocje)[24]. Należy mieć także na uwadze zachowanie klienta zlecającego przeprowadzenie nietypowej transakcji lub przeprowadzenie transakcji z braku oczywistych powodów, co może wskazywać na próbę nadużycia produktu lub usługi IO w celu dokonania przestępstwa ML lub FT. Uwagę przedstawiciela IO powinny zwrócić: zdenerwowanie klienta w sytuacji zadawania wnikliwych pytań związanych z prowadzoną działalnością; brak wiedzy klienta na temat prowadzonej działalności gospodarczej; nieznajomość przepisów prawa, uwarunkowań technicznych w obszarze ściśle powiązanym z jego celem realizacji, nietrzeźwość klienta w kontakcie z przedstawicielem IO; próba ukrycia twarzy; przychodzenie klienta do IO w towarzystwie osób trzecich i zachowywanie w tej sytuacji bierności; nietypowy transport gotówki

[23] *Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*.

[24] Analiza behawioralna łączy w sobie ocenę zachowań zewnętrznych (tzw. publiczne, czyli dostępne obserwacji z zewnątrz) i zachowań wewnętrznych (tzw. prywatne, czyli dostępne jedynie osobie, która ich doświadcza; należą do nich emocje, reakcje fizjologiczne organizmu, myśli). Obejmuje także interpretację zachowań i poznanie przyczyn. Analiza zachowań (wywodząca się z radykalnego behawioryzmu) koncentruje się natomiast na bezpośrednich obserwacjach i pomiarach określonej aktywności. W analizie zachowania wyodrębniły się trzy działy: eksperymentalna analiza zachowania (ang. *experimental analysis of behavior*), stosowana analiza zachowania (ang. *applied behavior analysis*) oraz konceptualna analiza zachowania (ang. *conceptual analysis of behavior*). W konsekwencji, wbrew temu, co głosi większość koncepcji psychologicznych, zachowania prywatne, takie jak myśli czy emocje, nie mogą być przyczyną zachowań publicznych, gdyż same wymagają wyjaśnienia w kategoriach przyczynowo-skutkowych. Zob. szerzej: P. Bąbel, *Terapia behawioralna zaburzeń rozwoju z perspektywy analizy zachowania*, „Psychologia Rozwojowa" 2011, t. 16, nr 3, s. 27–38. https://doi.org/10.4467/20843879PR.11.016.0189. W Polsce określenia analiza behawioralna i analiza zachowania są traktowane jako synonimy. Na potrzeby tego artykułu autor przyjął wskazane rozróżnienie między tymi pojęciami.

(reklamówki, torby podróżne itp.)[25]. W przypadku profilowania potencjalnego terrorysty samobójcy wyróżnia się takie cechy, jak: nerwowość, pocenie się, zachowanie jak po spożyciu narkotyków, rozszerzone źrenice, otępiały wzrok, pobudzenie, mało spójne zachowanie[26]. Podejrzane mogą być również: nietypowe wzorce transakcji, np. gdy klient kupuje identyczne przedmioty lub dokonuje kilku zakupów za tę samą kwotę; zmiany lokalizacji, np. gdy klient loguje się z nowego kraju lub regionu (szczególnie podejrzane jest, gdy klient loguje się z państwa trzeciego wysokiego ryzyka[27]); podejrzane próby logowania, np. gdy klient zmienia hasło kilka razy lub nie udaje mu się zalogować, klient wykazuje nietypowe wzorce pisania lub gesty dotykowe; zmiany w informacjach użytkownika, np. gdy klient podaje nowy adres wysyłki, numer telefonu, metodę płatności itp.[28] Ze wskazanych przykładów może wynikać to, że kryteria behawioralne w ocenie ryzyka ML/FT służą nie tyle budowaniu portretu psychologicznego, ile ocenie zachowania, które może świadczyć o sprzeczności między deklarowanym IO celem relacji a jej ukrytym celem przestępczym. Na podstawie dynamicznej oceny ryzyka IO może wysnuć także wnioski na temat zachodzących w czasie zmian w zachowaniu

[25] M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, wyd. 1, stan prawny na 12 maja 2013 r., Warszawa, s. 126.

[26] K. Liedel, *Profilowanie sprawców przestępstw terrorystycznych*, w: *Profilowanie kryminalne*, J. Konieczny, M. Szostak (red.), Warszawa 2011, s. 199. Tego rodzaju zachowanie należałoby rozpatrywać w przypadku samofinansowania się terrorysty samobójcy. Z badań przeprowadzonych przez Ariela Merariego wynika, że u większości zamachowców samobójców nie stwierdzono żadnego z czynników ryzyka kojarzonych z samobójstwem, takich jak: zaburzenia nastroju, schizofrenia, nadużywanie substancji lub wcześniejsze próby samobójcze. Zob. szerzej: A. Merari, *Academic research and government policy on terrorism*, „Terrorism and Political Violence" 1991, t. 3, s. 88–102. Ten wynik badań tłumaczony jest tym, że zamachowcowi samobójcy nie chodzi w ostateczności o dokonanie samobójstwa, ponieważ celem jest realizacja idei: męczeństwa, religijnej, społecznej.

[27] Zgodnie z art. 2 ust. 2 pkt 13 ustawy o p.p.p.f.t./2018 przez państwo trzecie wysokiego ryzyka rozumie się: „państwo identyfikowane na podstawie informacji pochodzących z wiarygodnych źródeł, w tym raportów z ewaluacji krajowych systemów przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu przeprowadzanych przez Grupę Specjalną do spraw Przeciwdziałania Praniu Pieniędzy (FATF) oraz organy lub organizacje z nią powiązane, jako nieposiadające skutecznego systemu przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu lub posiadające znaczące braki w systemie przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu, w szczególności państwo trzecie zidentyfikowane przez Komisję Europejską w akcie delegowanym przyjętym na podstawie art. 9 dyrektywy 2015/849". Zob. *Rozporządzenie delegowane Komisji (UE) 2016/1675 z dnia 14 lipca 2016 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849 przez wskazanie państw trzecich wysokiego ryzyka mających strategiczne braki*. Dla przykładu do takich krajów UE zalicza się: Koreę Północną, Iran, Algierię, Angolę, Wybrzeże Kości Słoniowej, Kenię, Laos, Liban, Monako, Namibię, Nepal, Wenezuelę.

[28] O. Skrebneva, A. Abramova, *Why Behavioral Analytics is Key to Fraud Detection Today*, The Sumsuber, 14 V 2024 r., https://sumsub.com/blog/behavioral-analytics/ [dostęp: 24 XI 2024].

klienta typowanego jako osoba udzielająca pomocy terrorystom. W konsekwencji wnioski mogą dotyczyć zmienności w czasie rodzaju pomocy udzielanej terrorystom czy jej zmniejszeniu lub intensyfikacji. To z kolei może wskazywać na typowanie miejsca zamachu, przygotowywanie aktu terrorystycznego lub zmianę geograficzną miejsca aktywności organizacji. Indywidualny profil behawioralny klienta powinien zostać wypracowany w ramach KYC[29]. Co istotne, jest to dana, która może być wygenerowana jedynie przez klienta i przez jego udział w relacji z IO. Sprawcą działań przestępczych może być także osoba trzecia niebędąca klientem IO (np. inspirator, akolita terrorystyczny, beneficjent rzeczywisty, osoba kontrolująca podmiot gospodarczy uwikłany w finansowanie aktywności terrorystycznej), pod wpływem której może działać klient. W takim przypadku klient będzie odgrywał rolę tzw. słupa („muła")[30], podmiotu zależnego, niekiedy osoba trzecia będzie kierowała jego zachowaniem. W tym przypadku należałoby oceniać zachowanie klienta w kontekście tego, na ile jest ono autonomiczne, a na ile zostało mu nakazane w relacji z IO. Przy definiowaniu nietypowych i nieuzasadnionych transakcji oraz zachowań klientów, przedstawiciel IO powinien wziąć pod uwagę dwa aspekty:

- nietypowe lub nieuzasadnione zachowanie klienta w kontekście oferowanego produktu lub usługi albo w kontekście rodzaju klienta,
- nietypowy lub nieuzasadniony charakter zachowania klienta wobec informacji, jakie IO ma na jego temat[31].

Ocena zachowania klienta stanowi element szerszego procesu kontroli klientów w danej IO i może stanowić element profilowania klienta. W rozważaniach odnoszących się do realizacji obowiązków IO należy założyć, że instytucja ta działa zgodnie z zapisami ustawy o p.p.p.f.t./2000, czyli poza rozważaniami pozostaje sytuacja, w której np. przedstawiciel IO świadomie współpracuje z klientem w ramach działań przestępczych.

---

[29] W konsekwencji jest budowany wzorzec normalnego zachowania klienta, który jest uzyskiwany za pomocą oceny zachowań transakcyjnych klienta w poprzednich okresach monitoringu przez IO.

[30] Rekrutacja „mułów finansowych" odbywa się najczęściej przez internet. Przestępcy kuszą łatwymi zarobkami i opisują oferowaną „pracę" jako bezpieczne, nieskomplikowane zajęcie. Takie propozycje trafiają głównie do osób szukających szybkiego dochodu. Osoby te często nie zdają sobie sprawy, że biorą udział w nielegalnym procederze, a ich konto bankowe staje się narzędziem wykorzystywanym do prania pieniędzy. Zob. *„Muły finansowe" – ukryte zagrożenie w świecie bankowości online*, prnews.pl, 2 XII 2024 r., https://prnews.pl/muly-finansowe-ukryte-zagrozenie-w-swiecie-bankowosci-online-481242 [dostęp: 12 X 2025].

[31] *The definition of unusual and unjustified transactions from the perspective of the risk of money laundering and terrorist financing*, https://www.cnb.cz/export/sites/cnb/en/faq/galleries/definition_of_unusual_and_unjustified_transactions_from_the_perspective_of_the_risk_of_money_laundering_and_terrorist_financing.pdf [dostęp: 14 III 2024].

W badaniach zachowania klienta w kontekście systemu AML/CFT należy zatem wziąć pod uwagę następujące czynniki:

- naturalne zachowanie człowieka wynikające z jego wykształcenia, środowiska, chorób, doświadczeń itp.;
- świadomie „sztucznie" wykreowane zachowanie człowieka, będące wynikiem uczenia się wzorca postępowania, naśladownictwa, chęci bycia innym, utożsamiania się z określoną postacią rzeczywistą lub fikcyjną[32];
- szczególne zachowania klienta w sytuacji mogącej świadczyć o jego udziale w zdarzeniu będącym elementem ML/FT (mieści się w tym zarówno zainspirowanie się do zachowania przestępczego i przygotowanie do przestępstwa, w tym w zakresie jego finansowania)[33].

Tym samym na potrzeby AML/CFT można wyróżnić czynniki behawioralne charakteryzujące:

- klienta zarówno standardowego, jak i niestandardowego (z ang. *customer behavioral factors*), np. czynniki behawioralne charakterystyczne dla klientów dokonujących zakupu na kredyt budynków ekologicznych (np. jako zachowanie konsumpcyjne);
- klienta kryminalnego (z ang. *behavioral factors of a criminal client*), w tym klienta zamieszanego w proceder ML i FT (z ang. *behavioral factors of the client of money laundering and terrorism financing*)[34].

Oceny ryzyka ML/FT, przyznawane podczas onboardingu, powinny być aktualizowane. Statyczne podejście oznacza, że nawet gdy zachowanie klienta zmieni

---

[32] W ramach funkcjonowania w grupie terrorystycznej takie zachowanie może być wynikiem społeczno-psychologicznym zgodnym z procesem związanym z radykalizacją, do których należą: grupa własna i/lub obca, konformizm, zgodność, myślenie grupowe, polaryzacja grupowa i dyfuzja odpowiedzialności. Zob. szerzej: D. Aziz Sbeih, *Which Group has a More Sustainable Model of Terrorism*, https://washingtoncollegereview.files.wordpress.com/2019/09/sbeih_which-group-has-a-more-sustainable-model-of-terrorism-al-qaeda-or-isis.pdf [dostęp: 24 XI 2024].

[33] Ta kwestia może być istotna w przypadku tzw. samotnych wilków, czyli terrorystów działających samotnie, bez powiązań z organizacją czy zleceniodawcą. To oznacza, że klient spełnia dwa warunki celowe – bycie inspiratorem i jednocześnie wykonawcą modelu zachowania wobec IO.

[34] Na potrzeby AML/CFT analiza behawioralna może być poszerzona o analizę pracowników IO, zwłaszcza w kontekście możliwości ich współdziałania z klientem w procederze prania pieniędzy. Zob. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*, art. 299 § 2: „Karze określonej w § 1 podlega, kto będąc pracownikiem lub działając w imieniu lub na rzecz banku, instytucji finansowej lub kredytowej lub innego podmiotu, na którym na podstawie przepisów prawa ciąży obowiązek rejestracji transakcji i osób dokonujących transakcji, przyjmuje, wbrew przepisom, środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, dokonuje ich transferu lub konwersji, lub przyjmuje je w innych okolicznościach wzbudzających uzasadnione podejrzenie, że stanowią one przedmiot czynu określonego w § 1, lub świadczy inne usługi mające ukryć ich przestępne pochodzenie lub usługi w zabezpieczeniu przed zajęciem".

się, np. gdy przejdzie on z realizacji przelewów krajowych na przelewy międzynarodowe lub będzie zaangażowany w sektory wysokiego ryzyka – nadal może być traktowany jako klient niskiego ryzyka. Dla zmiennego w czasie zachowania klienta powinna być zalecana dynamiczna analiza ryzyka ML/FT. To podejście powinno być adekwatne do zmian, które zaszły w osobowości klienta, i zaistniałych czynników zewnętrznych. Ta zmienność w czasie może świadczyć o angażowaniu się klienta w działalność niezgodną z prawem. Według Brytyjskiego Urzędu Nadzoru Finansowego (Financial Conduct Authority, FCA) modele scoringu ryzyka powinny uwzględniać pojawiające się zagrożenia, zmiany w zachowaniach klientów oraz aktualizacje ram regulacyjnych[35].

Nowi klienci, którzy chcą wejść w relacje z IO, aby dokonywać przestępstw, mogą zachowywać się specyficznie, np. unikać kontaktu z instytucją lub znacznie go minimalizować. W przypadku oferowania usług online instytucja podejrzewająca możliwość wystąpienia nietypowych zachowań, powinna wprowadzić innego rodzaju czynniki identyfikujące te zachowania. Do takich zachowań można zaliczyć: brak odpowiedzi na pytania dotyczące klienta, jego firmy, brak skonkretyzowania beneficjenta ostatecznego (rzeczywistego), zakłopotanie klienta, zdenerwowanie, potrzebę natychmiastowej konsultacji z osobą trzecią lub nawet groźby co do naruszania podstawowych praw klienta i konsekwencji takiego zachowania. Instytucja powinna rozważyć, czy nie jest to podejrzane, szczególnie jeśli klient może mieć powiązania przestępcze lub ma nietypową wiedzę na temat procesu ML.

Jak zauważa Jacek Grzywacz, segmentacja klientów jest możliwa także przez poznanie sposobu postrzegania oferty przez nabywcę: *Przy wykorzystaniu tego kryterium można określić reakcję klienta na cenę usług finansowych, jego gotowość korzystania z tzw. ofert specjalnych oraz preferowany sposób dystrybucji usługi (np. za pośrednictwem bankowości elektronicznej)*[36]. Biorąc pod uwagę cel oferty i potrzeby klienta, można konfrontować jego zachowanie z przyjętym w IO wzorem oferty, wobec realizacji potrzeb i celu zgodnie z wprowadzonym modelem instrumentu na rynek finansowy, a także działaniami niezgodnymi z jej przeznaczeniem i deklarowanym celem. W ten sposób tworzy się pewien zbiór nietypowych zachowań klienckich (osąd konsumenta), które należałoby poddać identyfikacji w zakresie AML/CFT. W przypadku tzw. identyfikacji na odległość, dotyczącej głównie informacji, dokumentów, danych, jakimi będzie posługiwał się klient w relacji z IO, traci się czynnik ocenny w postaci behawioralnych reakcji klienta. Działanie na odległość

[35] *Guidance for a Risk-Based Approach the Banking Sector*, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf [dostęp: 20 I 2025].

[36] J. Grzywacz, *Segmentacja na rynku usług bankowych*, „Zeszyty Naukowe PWSZ w Płocku. Nauki Ekonomiczne" 2014, t. 20, s. 44.

umożliwia monitorowanie klienta pod względem sposobu korzystania z urządzeń mobilnych, np. sposobu logowania się, pomyłek we wprowadzaniu kodu, szybkości i sposobu pisania znaków w korespondencji z instytucją.

Wykorzystanie podejścia behawioralnego na potrzeby identyfikacji nietypowych zachowań klienta

Istotnym elementem podejścia behawioralnego w AML/CFT pozostaje badanie pozostawionego „śladu" behawioralnego[37] klienta zarówno na poziomie bezpośredniej, fizycznej relacji z IO, jak i podejmowanej na odległość. Do ocenianych zachowań klienta zalicza się: niechęć do podawania danych identyfikacyjnych lub podawanie ich w sposób okrojony, dotyczy to także podmiotów reprezentujących; zgadzanie się na wysokie kary; dokonywanie transakcji bez logicznego uzasadnienia; zlecanie transakcji po uprzednim uzyskaniu środków z nieustalonych lub trudnych do ustalenia źródeł[38]. Śladami wobec czynności IO będą wszelkie zmiany w obiektywnej rzeczywistości, zbliżające je do oceny kryminalistycznej. Instytucja obowiązana nie korzysta np. z wariografu, powinna więc zapewnić sobie możliwość ujawnienia i identyfikacji śladów zachowania behawioralnego w celu identyfikacji klienta oraz pozyskania wiedzy na jego temat. Co istotne, w przypadku aktywizowania się klienta będzie niezbędne dokonanie oceny jego poczucia skuteczności w dokonywaniu przestępstwa lub postrzeganej kontroli zachowania. Istotny może być wyróżnik czasowej korelacji działania z dokonaniem przestępstwa, a także ocena psychicznej więzi z przestępstwem wyrażonej w zachowaniu klienta-sprawcy[39]. Może to być np. postawa obojętna, towarzysząca etapowi przygotowań do popełnienia przestępstwa np. przez podpisanie umowy o prowadzenie rachunku bankowego, rozważaniu oferty usług związanych z tym rachunkiem, czy jako relacja z IO w stanie wewnętrznego doradztwa. Zachowanie klienta może być inne, gdy zależy mu na czasie realizacji usługi, szybkości dokonania przelewu, realizacji transakcji okazjonalnej, zwłaszcza gdy będą w tym zakresie zachodziły dodatkowe czynniki zwiększające ryzyko, np. transfer środków do kraju trzeciego UE, kraju ościennego wobec aktywności terrorystycznej czy kraju identyfikowanego ze słabym systemem bezpieczeństwa prawnego i wysokim stopniem zagrożenia przestępczością. W tym zakresie

[37] Zob. szerzej: K. Olszak-Häußler, *Rozumienie pojęcia „ślad" w ujęciu profilowania kryminalnego*, „Problemy Kryminalistyki" 2016, nr 291, s. 7–11.

[38] *Risk assess your business for money laundering supervision*, Gov.UK, 23 X 2014 r., https://www.gov.uk/guidance/money-laundering-regulations-risk-assessments [dostęp: 18 XI 2024].

[39] Zachowanie człowieka musi uzewnętrznić się w obiektywnej rzeczywistości.

należałoby także wziąć pod uwagę umiejętności[40] klienta do realizacji negatywnych działań. Co ważne, mimo że IO powinna zmierzać do ustalenia nieprawidłowości w celu wykazania przestępstwa z art. 299 i 165a Kodeksu karnego (k.k.)[41], to nie mówi się o potrzebie wykazania, a tym bardziej udowodnienia, przez IO winy klienta – potencjalnego sprawcy. Tym samym instytucji badającej zachowanie klienta nie dotyczy procedura karna. Dlatego też może badać zachowanie klienta i/lub sprawcy obejmujące cechy niezwiązane z dobrem prawnym chronionym przez normę sankcjonowaną, która leży u podstaw tego typu czynu zabronionego. W odniesieniu do ustaleń w IO ustawodawca aktualnie mówi wprost o okolicznościach, mogących wskazywać na podejrzenie popełnienia przestępstwa, a nie o winie klienta typowanego jako sprawca (art. 74 ust. 1 ustawy o p.p.p.f.t./2018). Winę należy rozpatrywać w odniesieniu do czynu zabronionego, a nie do cech osobowościowych, charakteru i trybu życia klienta i/lub sprawcy. Okoliczności wskazujące na podejrzenie popełnienia przestępstwa mogą obejmować także ocenę tych elementów, o ile będą służyły wskazaniu podejrzanych działań. Ponadto nie muszą być zawężone jedynie do czasu popełnienia czynu, ale powinny go uwzględniać jako punkt odniesienia. Rozpoznanie skupia się na zachowaniu klienta, a dopiero później na tym, co zrobił lub czego mógł dokonać. Karane zachowania sensu stricto zostały wskazane w art. 299 § 1 k.k.:

> Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

oraz w art. 165a § 1 k.k.:

> Kto gromadzi, przekazuje lub oferuje środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości w zamiarze sfinansowania przestępstwa o charakterze terrorystycznym lub przestępstwa, o którym mowa w art. 120,

[40] Jedną z nich może być przyjęcie przez klienta postawy, że może on wprowadzić w błąd przedstawiciela IO co do rzeczywistego motywu nawiązania relacji z instytucją. Tu także można rozważyć identyfikację złośliwej aktywności, przy użyciu tego, co nazywa się wykrywaniem opartym na regułach, w którym obserwowane zdarzenia są dopasowywane do znanych modeli zachowań zagrażających.

[41] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*.

art. 121, art. 136, art. 166, art. 167, art. 171, art. 252, art. 255a lub art. 259a, podlega karze pozbawienia wolności od lat 2 do 15.

Zachowania te zostały potraktowane odmiennie ze względu na cel dokonania przestępstwa. W przypadku ML jest to zapewnienie legalności dochodów z czynów zabronionych a w przypadku FT – przekazania środków na rzecz (zwłaszcza innego podmiotu) beneficjenta terrorystycznego (wyjątek stanowi samofinansowanie). Stąd też wobec ML stwierdza się cykliczność zachowania, a w przypadku FT – jego liniowy charakter[42].

W związku z przedmiotowymi rozważaniami można rozważyć podział na behawiorystykę dotyczącą:

- czynu przestępnego – ocena zachowań osoby pod kątem popełnienia czynu karalnego (art. 299 k.k., art. 165a k.k.) jako wypełnienie strony przedmiotowej przestępstwa;
- relacji podejrzanej – ocena zachowań osoby w relacji z IO świadczących o okolicznościach wskazujących na podejrzenie ML/FT lub postąpienia z aktywem w sposób, który uzasadnia podejrzenie, że określona transakcja lub wartości majątkowe mogą mieć związek z ML/FT;
- świadczonych usług i/lub produktów z wyłączeniem dwóch poprzednich. Dotyczy to zachowań wobec podmiotów nadzorowanych i nienadzorowanych czy świadczeń rejestrowanych i nierejestrowanych, np. relacji z przedstawicielem punktu obsługującym system hawala.

Założeniem zastosowania oceny behawioralnej klienta może być to, że zachowania sprawców w zakresie ML/FT są poznawalne i powtarzalne. Celem ML jest zalegalizowanie środków pochodzących z czynu zabronionego, a w przypadku finansowania terroryzmu chodzi o wsparcie aktywności terrorystycznej. Można zatem mieć do czynienia z zachowaniami podobnymi, a w niektórych fazach działania zachowania te mogą być tożsame dla ML i FT. Trudne jest zatem uzyskanie specyficznego wyróżnika, który mógłby zwrócić uwagę decydentom w pionie AML/CFT i komórkach współpracujących w IO na możliwość działań przestępczych. Wyróżnikiem w tym zakresie może być ocena behawioralna zachowania klienta jako sprawcy. O ile jednak scenariusze i taktyka są znane, a nawet mogą być przewidywalne, o tyle sprawcy znacznie różnią się między sobą pod względem cech indywidualnych (nie ma dwóch osób o tych samych cechach osobowościowych), a także bodźców, pod których wpływem działają. Sprawcy mogą posługiwać się pewnym wyodrębnionym pakietem instrumentów, ale jest to połączone z innym

[42] *Comparison: Terrorist Financing, Money Laundering, and Financing…*; *Counter Proliferation Financing. Guidance Notes…*

rodzajem dokonywanych przez nich działań (zdominowanym przez cechy indywidualne). Ta cecha wyróżniająca i indywidualizująca osobowość klienta może ujawnić udział klienta w procederze, a także pomóc monitorować jego zachowania na odległość. W konsekwencji IO w ramach KYC będzie musiała pozyskać wiedzę co do zachowania klienta, który daje wzorzec behawioralny. To podejście może być pomocne zwłaszcza wtedy, gdy relacje klient – IO mają trwać przez dłuższy czas oraz gdy IO zaoferowała klientowi produkt dostępny online. Pozyskanie KYC behawioralnego, zwłaszcza uwzględniającego zaburzenia, może być przydatne do typowania klienta jako terrorysty, który może realizować plan samofinansowania swojego czynu (np. dąży do uzyskania wysokiego poziomu autonomii w relacji z IO oraz w zakresie zawiadywania udostępnionymi produktami czy usługami). W takim przypadku poszukuje się nieznanego sprawcy, ale obserwacja behawioralna może pozwolić na zidentyfikowanie ryzyka. Wskaźnikiem ryzyka jest np. działanie klienta na forach internetowych poświęconych szerzeniu zachowań ekstremistycznych.

Właściwą praktyką poprzedzającą ocenę zachowań klientów typowanych jako potencjalni sprawcy ML/FT byłoby poznanie mechanizmów psychologicznych związanych ze sprzedażą produktów oferowanych przez daną IO[43]. Dzięki temu przedstawiciel instytucji będzie wiedział, jak powinni się zachowywać standardowi klienci wobec oferowanych produktów, i rozpozna odchylenia od ustalonych wzorców sprzedaży. Można w tym celu wykonać testy, np. test DISC[44] obejmujący cztery główne kategorie, według których można analizować osobę. Są to style zachowania:

1) dominujący – określa on, jak ludzie patrzą na wyzwania i przeszkody. Osoby, u których ta cecha przeważa, są zorientowane na cel i mają zdecydowane opinie,
2) wpływowy – charakteryzuje ludzi, którzy są pewni siebie i otwarci na pomysły. Takie osoby wywierają wpływ na otoczenie – inspirują innych swoimi pomysłami,
3) stabilny – wskazuje, jak dana osoba reaguje na otoczenie. Ludzie o tej cesze są dobrymi słuchaczami, są spokojni, cenią stałość,
4) sumienny – wskazuje, jak ludzie reagują na daną sytuację. Takie osoby są analityczne, przy podejmowaniu decyzji opierają się przede wszystkim na wiedzy i faktach[45].

[43] Zob. szerzej: A. Falkowski, T. Tyszka, *Psychologia zachowań konsumenckich*, Gdańsk 2001.

[44] DISC (ang. *dominance*, *inducement*, *submission*, *and compliance*) to model czterech stylów zachowań, opracowany na podstawie badań amerykańskiego psychologa Williama Marstona.

[45] H. Sekar, *Recognize Your Customers: A Complete Guide on Customer Behavioral Cues and Building Customer Relationships*, 8 VII 2019 r., https://www.freshworks.com/freshdesk/customer-engagement/customer-behavioral-cues-building-customer-relationships-blog/ [dostęp: 12 III 2024].

Każdy człowiek jest kombinacją tych cech w różnym stopniu. Rozpoznając sygnały płynące od potencjalnych klientów, będzie można lepiej ich zrozumieć i nawiązać z nimi lepszy kontakt. Istotne jest ustalenie determinant, jakie mają wpływ na zachowanie klienta jako sprawcy. Przy czym wszechstronne zastosowanie KYC pozwoli na zbudowanie określonego obszaru poruszania się w ramach rozpoznawania klienta, a tym samym podejście behawioralne będzie łatwiejsze. Będzie się ono skupiało wyłącznie na relacji zachowanie klienta – typowanie klienta jako sprawcy przestępstwa (identyfikacji klienta jako uwikłanego w okoliczności mogące świadczyć o podejrzeniu ML/FT lub budzącego uzasadnione podejrzenie, że jego działanie jest nakierowane na użycie środków i/lub transakcji do ML/FT). Działania IO mają na celu rozpoznanie konfiguracji zdarzeń i uczestnictwa w nich klienta i są prowadzone w związku z potrzebą ustalenia ryzyka zachowań niezgodnych z prawem oraz wyciągnięcia wniosków, które w formie określonej prawem należy następnie przekazać do jednostki analityki finansowej. Istotne jest wyeliminowanie z oceny tych determinant podejrzanego zachowania sprawcy, które są powiązane z innymi przyczynami (np. zachowania socjopatyczne, niska samoocena, niesprawność intelektualna, depresja, zażywane leki itp.) i nie są zachowaniami kwalifikującymi klienta jako potencjalnego sprawcę przestępstwa ML/FT. Ostatecznie pozostają do oceny jedynie te determinanty, które będzie można powiązać z nietypowym zachowaniem sprawcy, kwalifikującym go jako podejrzanego o udział w procederze przestępczym. Decydent w IO powinien dążyć w KYC behawioralnym do zachowania jedynie tych determinantów, które są istotne w zachowaniu sprawcy, typowane jako obarczone podejrzalnością. Pozostałe mogą być wynikiem różnych przypadłości, braku doświadczenia czy wstydliwości, choroby, niskiego poziomu wykształcenia, braku wiedzy na temat znajomości mechanizmów rynkowych. Nie będą one jednak pozostawały w związku przyczynowo-skutkowym z rolą, jaką klient odgrywa w procederze ML/FT. Wobec powyższego można wywnioskować, że sprawca może być osobą:

- mającą cechy przynależne skutecznemu dokonaniu przestępstwa ML/FT za pomocą produktów czy usług oferowanych przez IO,
- wywodzącą się z kręgów przestępczych (a tym samym cechującą się pewnymi zachowaniami dyssocjalnymi), która została wykorzystana do realizacji procederu ML/FT,
- niemającą konfliktu z prawem, która została wybrana do odegrania aktywnej roli w procederze ML/FT ze względu na cechy osobowościowe,
- samorealizującą się w roli podmiotu zarówno dokonującego przestępstwa, jak i finansującego je.

Aby uzyskać wiedzę na temat skłonności klienta do działania pod wpływem określonych czynników (np. takich jak uzyskiwane dochody, zasoby finansowe, sytuacja materialna, upodobania, promocje, ale także indywidualne cechy charakteru

i usposobienia), należy przede wszystkim z nim porozmawiać. Pozwoli to na poznanie nie tylko jego oczekiwań wobec IO, lecz także przewidzenie zachowań jako potencjalnego partnera w relacjach z instytucją. Przedstawiciel IO może mieć przewagę nad klientem, ponieważ powinien lepiej znać oferowane produkty czy usługi i znać ich atrybuty[46], zgodnie z celami polityki komercyjnej[47], biznesowej przyjętymi w IO. Może mu to pomóc w ocenie klienta i sformułowaniu wniosków dotyczących jego zachowania w czasie składania oferty. Pomocne będzie także doświadczenie w zakresie psychologii sprzedaży i rozmowy z klientem. Podmiot monitorujący powinien mieć wiedzę, która pozwoli mu ocenić indywidualne predyspozycje klienta do ML/FT. Rozmowa powinna ujawnić jego motyw do nawiązania relacji z takim rodzajem IO oraz uzyskania dysponowania określonym produktem lub korzystania z określonej usługi. W przedstawionej relacji klient – IO chodzi także o to, aby IO nie popełniła błędu polegającego na złożeniu klientowi nieodpowiedniej oferty, niezgodnej z jego oczekiwaniami. Skutki takiego błędu IO mogą zostać sklasyfikowane jako niewłaściwe zachowanie klienta. Dobór klienta może mieć także podłoże ekonomiczne, ale w przypadku działań ML/FT będzie on motywowany np. możliwością podania ograniczonej liczby danych osobowych i innych danych szerzej identyfikujących klienta, ograniczeniami instytucji w dostępie do baz danych, które pozwoliłyby głębiej zweryfikować klienta, możliwością szybkiego transferu środków zarówno w kraju, jak i za granicą, możliwością skorzystania z pakietu różnych usług, szerokimi możliwościami dysponowania środkami bez potrzeby fizycznej obecności w siedzibie instytucji, rodzajem obsługiwanych klientów, z którymi klient się utożsamia lub do których się upodabnia w zachowaniu, kierowaniem się negatywnymi opiniami o instytucji zamieszczonymi w mediach publicznych i społecznych.

Zachowanie przestępcze jest postrzegane przez behawiorystów jako wyuczona reakcja na bodźce środowiskowe, a nie wynik wrodzonej osobowości lub cech charakteru. Zachowania te są wzmacniane przez nagrody, takie jak zdobycie pieniędzy lub władzy, czy unikanie negatywnych konsekwencji, takich jak kara lub

[46] Atrybuty to określone właściwości produktu, które służą do jego opisu i klasyfikacji, ale nie wpływają bezpośrednio na cenę czy dostępność produktu. Wobec produktów finansowych bierze się pod uwagę takie cechy, jak: ryzyko, czas trwania, potencjalne korzyści, stopa zwrotu oraz rodzaj instrumentu (np. akcje, obligacje, lokata), które odróżniają go od innych i pozwalają na ocenę jego wartości dla klienta. Oprócz specyficznych cech produktu, na jego postrzeganie wpływają także atrybuty o charakterze niematerialnym, m.in. wizerunek marki, jakość obsługi klienta. Zob. Di Wu, Xuhui Li, *A Systematic Literature Review of Financial Product Recommendation Systems*, „Information" 2025, nr 16. https://doi.org/10.3390/info16030196.

[47] Dotyczy działania firm, które mają na celu zwiększenie ich zysków przez np. agresywne promowanie produktów czy ustalanie cen.

dezaprobata społeczna[48] (nie jest wyjątkiem nakłanianie kogoś do popełnienia przestępstwa w zamian za określoną kwotę lub udział w zyskach). To podejście łączy się z istotnym założeniem behawioryzmu, którym jest zewnętrzna sterowność człowieka. Dlatego w ramach AML/CFT należy ocenić, czy podmiot pozostający w relacji z IO jest osobą, za którą się podaje, czy działa z własnej woli, czy też za tym działaniem stoi inny podmiot. Może tak być w sytuacji, gdy dana osoba podaje się za kogoś innego (np. w wyniku wyłudzenia danych), gdy przestępstwo jest dokonywane na tzw. słupa oraz gdy za osobą wykonawcy ukrywa się cichy udziałowiec lub rzeczywisty beneficjent. Nie są to przypadki odosobnione i nie dotyczą tylko przestępczości związanej z ML czy FT. To zastrzeżenie jest o tyle ważne, że przedstawiciel IO w ramach obowiązków AML/CFT powinien nie tylko rozpoznać sytuację, w której doszło do takiego zdarzenia, lecz także dokonać jego subsumpcji na potrzeby zidentyfikowania celu tożsamego z celem dla przestępstwa ML i FT. Istotą oceny staje się postawienie pytania, czy dana osoba wchodząca w relacje z IO działa z własnej woli, czy jej zachowanie stanowi reakcję na bodziec zewnętrzny lub jest wynikiem zależności. Drugie pytanie dotyczy tego, czy i w jakim zakresie takie działanie przekłada się na skalę ryzyka i na rodzaj niezbędnych do zastosowania środków bezpieczeństwa finansowego[49].

Nie należy zakładać, że klient zaangażowany w proceder ML/FT popełni błąd. Sprawca będzie się starał unikać błędów, które mogłyby ujawnić jego złe intencje, lub pozostawiać fałszywe ślady, aby wprowadzić w błąd decydenta w IO. Może on tworzyć scenariusze alternatywne, mieć zdolności do perfekcyjnego odegrania roli w relacji z IO, być odporny na stres i prawidłowo postępować pod presją czasu, mieć zdolności manipulacji psychologicznej czy predyspozycje do takiego postępowania[50]. Może być zdeterminowany do osiągnięcia celu w sposób przemyślany i logiczny (zgodnie z opracowanym lub nabytym algorytmem postępowania), umiejętnie odegrać swoją rolę standardowego klienta wobec przedstawiciela IO, zastosować metody socjotechniczne i manipulację[51], mieć wiedzę z zakresu finansów i gospodarki, odporność psychiczną na błędy i zniekształcenia poznawcze (zazwyczaj popełniane pod

[48] A.J. McKee, *behaviorism | Definition*, Doc's CJ Glossary, https://docmckee.com/cj/docs-criminal-justice-glossary/behaviorism-definition/ [dostęp: 12 III 2024].

[49] Ocena dotyczy jedynie relacji klient – IO. Nie można wykluczyć, że sprawdzenie zachowań transakcyjnych będzie powiązane ze sprawdzeniem innych rodzajów zachowań, np. kontaktu z mediami w celu powiadomienia o planowanym zamachu, przyznania się do dokonania aktu terrorystycznego.

[50] Członkowie grup terrorystycznych stosują zabiegi socjotechniczne na potrzeby werbowania zwolenników i przekonywania do swoich podglądów oraz radykalnych metod ich wdrażania w relacje społeczne (np. sprawowania kontroli nad zwolennikami). Dlatego też te zabiegi mogą mieć przełożenie na relacje z IO.

[51] Tym samym nie będzie można właściwie i adekwatnie do zagrożenia wyprofilować i ocenić ryzyka.

wpływem emocji) czy zdolności do konfabulacji. Niestety w przypadku oceny zachowania sprawcy określonego w art. 165a § 4 k.k. (popełnienie czynu zabronionego w sposób nieumyślny) sprawa może być problematyczna. Zachowania, które przedstawicielowi IO mogą się wydać niewłaściwe, mogą wynikać z braków intelektualnych i społecznych sprawcy lub z konfrontacji ze skomplikowanymi w jego ocenie czynnościami i decyzjami, jakie należy podjąć, aby zrealizować cel przestępczy, a jednocześnie nie ujawnić prawdziwego motywu postępowania. Ponadto sytuacja, w jakiej się znalazł w relacji z danym rodzajem IO, może być dla klienta nowym doświadczeniem i zachowanie odpowiednie do okoliczności będzie niemożliwe. Brak samokontroli, niski poziom inteligencji emocjonalnej mogą spowodować użycie gestów i słów nieadekwatnych czy wyuczonych w przeszłości (np. ze środowiska przestępczego, więziennego, skrajnej ideologii terrorystów) i zdradzić rzeczywiste cele relacji nawiązywanej przez klienta. Może to ujawnić ukryty motyw relacji, zwłaszcza w sytuacji oferty kilku stanów dla podjęcia decyzji, i może przejawiać się zaprzestaniem logicznego postępowania w wyniku zmiany oferty ze strony IO czy coraz bardziej agresywnymi próbami podporządkowania sobie przedstawiciela IO. Błędne zachowanie może być także efektem braku zrozumienia lub niewłaściwego zrozumienia oferty złożonej przez instytucję, co zakłóca przygotowaną taktykę postępowania[52].

Przedstawiciel IO musi mieć także na uwadze możliwość wejścia w relację z tzw. zawodowym praczem środków[53], np. gdy nie zadziałały linie ochrony na poziomie: wykonawczym – compliance – zarządu, ale także gdy IO świadomie będzie

[52] To może dotyczyć sytuacji, w której klient powołuje się na podobne rozwiązanie efektywnie zakończone w relacji z inną instytucją, z jednoczesnym wyrażeniem dezaprobaty, że w aktualnym stanie relacji odmawia mu się pozytywnego zakończenia nawiązania relacji lub doprowadzenie do ich ustania. Zwłaszcza gdy za uzyskanie wymaganego wyniku w relacji z uprzednią instytucją otrzymał on nagrodę za skuteczne zrealizowanie znamion przestępczych.

[53] Profesjonalne pranie pieniędzy (ang. Professional Money Laundering, PML) „to zaawansowana forma działalności przestępczej, która polega na profesjonalnej pomocy w ukrywaniu pochodzenia, właścicieli i przeznaczenia nielegalnych dochodów. Jej celem jest wprowadzenie tego rodzaju funduszy do systemu finansowego w taki sposób, aby było to niewidoczne dla instytucji kontrolujących przepływ środków". Zob. szerzej: *Czym jest PML i jakie zagrożenie stanowi dla AML? Metody działania umożliwiające przestępcom profesjonalne pranie pieniędzy oraz strategie w walce z PML*, iaml, 6 X 2025 r., https://www.iaml.com.pl/wiedza/pml/ [dostęp: 12 X 2025]. Sprawcami są osoby, które czerpią korzyści z legalizacji środków pochodzących z przestępstw należących do innych osób. Za swoje „czynności legalizacyjne" otrzymują określoną prowizję. Profesjonaliści wykorzystują złożone struktury finansowe, firmy-słupy, waluty wirtualne i inne metody, aby ukryć ślady i ponownie włączyć pieniądze do legalnej gospodarki, doskonalą także stale swoje metody i uczą się nowych instrumentów rynków finansowych, aby doskonalić przestępcze przedsięwzięcia. Niejednokrotnie są też wykorzystywani na rzecz wspierania procederów kamuflowania procesów finansowania proliferacji. Zob. *FATF REPORT. Professional Money Laundering*, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf [dostęp: 12 X 2025].

wspierała taki podmiot. Tu może wystąpić zjawisko korupcji oraz pozytywna ocena korzyści i strat w przypadku ewentualnej kary pieniężnej dla IO. Takich sprawców charakteryzuje konieczność przestępczego działania (to ich sposób na pozyskanie środków do życia), potrzeba przynależności i bycia potrzebnym (do świadczenia usług przestępczych), potrzeba bycia szanowanym jako profesjonalista w kręgach przestępczych i realizacji własnego potencjału. To osoby, które są albo były członkami grupy przestępczej, które zmieniają swoje role i ryzykują narażeniem z postrzeganego przestępstwa „twardego" na bardziej wyrafinowany „białych kołnierzyków" lub osoby niezależne oferujące swoje usługi na rzecz przedstawicieli innego rodzaju przestępczości[54]. Takie osoby cechują się znajomością przepisów, biznesu, finansów, odważnym stawieniem problemu, ekspansywnością, mogą one sugerować podział zysków z decydentami z IO, oferować współdziałanie z IO (w tym składać oferty korupcyjne decydentom) w celu kamuflażu transakcji służących ML, aby nie doszło do ich ujawnienia. Tę kategorię sprawców zawodowych można podzielić na dwie grupy. Pierwsza to sprawcy ujawnieni, którzy nie kryją swojego przestępczego postępowania i jako oferenci lub pracownicy IO realizują je z premedytacją. Drudzy to ci, którzy nie ujawniają się wobec IO co do celu postępowania, a proceder prania pieniędzy doprowadzają do perfekcji. Sprawcy nieujawnieni mają tendencję do trzymania się działających metod i zmieniają je tylko wtedy, gdy te przestają działać lub stają się zbyt ryzykowne[55]. Potrafią także wychwycić luki wiedzy przedstawicieli IO i ich słabość psychiczną.

Nie oznacza to, że obserwację zachowań sprawców na potrzeby AML/CFT będzie można wykorzystać jedynie w relacji klient – IO. Należy zauważyć, że w ramach systemu AML/CFT funkcjonują inne podmioty zajmujące się zwalczaniem tych procederów. Podejście behawioralne będzie pomocne w realizacji zadań np. przez Straż Graniczną, współpracującą w celu identyfikacji osób, które mogą przemycać przez granicę m.in. gotówkę (ale także artefakty, dzieła sztuki czy inne produkty mogące być przedmiotem przestępstwa ML bądź FT). Zachowania behawioralne mogą być obserwowane również na potrzeby czynności dochodzeniowo-śledczych czy operacyjno-rozpoznawczych (np. w ramach prowadzenia przesłuchań czy współpracy z osobowym źródłem informacji). Jest to związane z tym, że ocena zachowania sprawcy musi opierać się na połączeniu oceny dotyczącej sfery wewnętrznej człowieka (psychiki) i oceny jego zachowań.

[54] D. Thomas, *Profiling Part 1: The Psychology of Anti Money Launderers*…, s. 6.

[55] D. Thomas, *Profiling Part 2: The Psychology of Anti Money Launderers*, https://www.world-check.com/media/d/content_whitepaper_reference/WhitePaper_The_Psychology_Of_Anti_Money_Launderers.pdf [dostęp: 28 XI 2024].

Niestety w ramach podejścia behawioralnego można mieć do czynienia z sytuacjami, w których pomiary ukrytego zachowania klienta mogą nie być możliwe. Tym samym obserwacja będzie dotyczyła tylko zachowania zewnętrznego klienta, bez możliwości klasyfikowania na tej podstawie jego myślenia i emocji. W tym przypadku można zastosować scenariusze alternatywne czy mikrosymulacje zdarzeń i obserwować, jak klient sobie radzi w tych sytuacjach. Takie działania wymagają wnikliwej znajomości oferowanego produktu czy usługi, umiejętności rozmowy z klientem i oceny jego zachowania z punktu widzenia psychologicznego. Takie podejście może być realizowane etapowo, aby móc ocenić, jak na danym etapie zachował się klient. Dzięki temu przedstawiciel IO będzie mógł skupić się przede wszystkim na tym etapie, na którym klient zachował się najbardziej nieracjonalnie na skutek zakłócenia przyjętego przez niego scenariusza przestępczego. Impulsem może być przedłożenie klientowi oferty strukturyzowanej[56] dalszego inwestowania za pośrednictwem innych usług świadczonych przez IO[57]. Reakcja przedstawiciela IO nie powinna być przesadzona, ponieważ instytucji powinno zależeć na utrzymywaniu relacji i kontynuowaniu obserwacji zachowania klienta. Dalsze działanie może wykluczyć jedynie spełnienie się przesłanek określonych w art. 41 ust. 1 ustawy o p.p.p.f.t./2018.

W ramach podejścia behawioralnego należałoby także przywołać teorię koncepcji człowieka ekonomicznego (łac. *homo oeconomicus*). Zakłada ona, że człowiek jako istota działająca racjonalnie zawsze dąży do maksymalizacji osiąganych zysków i dokonywania wyborów ze względu na wartość ekonomiczną rezultatów tych wyborów. Człowiek ekonomiczny, wybierając jakieś działanie spośród działań możliwych w danej sytuacji, decyduje się na to, dla którego przewaga korzyści nad stratami jest największa[58]. Zarówno przestępstwo ML, jak i FT nie są dokonywane

[56] Oferta strukturyzowana w bankach obejmuje produkty łączące bezpieczeństwo lokaty z potencjalnym zyskiem z inwestycji, gdzie część środków jest chroniona, a pozostała część – inwestowana w instrumenty finansowe, takie jak akcje, indeksy czy waluty.

[57] Na przykład: klient wykonujący co miesiąc tę samą transakcję mniej więcej w tym samym czasie (np. płacący czynsz lub media w dniu wypłaty) może zostać poproszony o utworzenie miesięcznego zlecenia stałego; klient, który przez długi czas miał na rachunku bieżącym niewykorzystane środki, może zostać poproszony o przelanie pieniędzy na wysoko oprocentowane konto oszczędnościowe; klient dokonujący płatności z oprocentowanego rachunku oszczędnościowego, gdy na rachunku bieżącym znajdują się wystarczające środki, może zostać poproszony o wykorzystanie środków na rachunku bieżącym bez utraty odsetek z konta oszczędnościowego. Zob. szerzej: S. Fernando, *Behavioral Authentication: Improving Security and CX Without Compromise*, WSO2, 21 VII 2023 r., https://wso2.com/library/whitepapers/behavioral-authentication-improving-security-and-cx-without-compromise/ [dostęp: 28 XI 2024].

[58] Zob. W. Załuski, *Założenie deskryptywne ekonomicznej analizy prawa: człowiek jako homo oeconomicus*, w: *System prawny a porządek prawny*, O. Bogucki, S. Czepita (red.), Szczecin 2008, s. 297 i nast.;

z chęci zysku. W pierwszym przypadku zysk w drodze czynu zabronionego już został osiągnięty. Celem jest uprawdopodobnienie tego, że pochodzi on z legalnych przedsięwzięć. W drugim przypadku chodzi o dostarczenie środków na realizację określonej idei metodami niezgodnymi z prawem (niejednokrotnie zyskiem są korzyści mentalne), tj. zasilenie materialne i finansowe sprawców i organizatorów aktów terrorystycznych. Tym samym podejście z uwzględnieniem zysków i strat może być przedmiotem oceny zachowania pod kątem behawioralnym, zwłaszcza w przypadku IO jako instytucji finansowych. Oznacza to, że gdy przedstawiciel IO wchodzi w relację z klientem – potencjalnym sprawcą ML/FT – nie uzyska wprost wiedzy o zamiarze nawiązania i prowadzenia relacji z instytucją. Ten zamiar jest ukrywany przez klienta ze względu na potrzebę zrealizowania przez niego taktyki przestępczej, tj. zalegalizowania środków z przestępstwa czy przesunięcia ich bliżej decydentów terrorystycznych i ich przestępczego wykorzystania w ramach przygotowania do zamachu lub utrzymania zabezpieczenia logistycznego. Ujawnienie mogłoby zakończyć się nienawiązaniem relacji lub ich ustaniem (zob. działanie w ramach de-riskingu), a także ograniczeniem dysponowania środkami na podstawie art. 86 ustawy o p.p.p.f.t./2018. Tym samym przedstawicielowi IO pozostaje jedynie prowadzenie oceny zachowania takiego klienta i jego odpowiednie stymulowanie lub oczekiwanie na popełnienie błędu. Ta obserwacja pozwoli także potwierdzić lub zaprzeczyć postawionej tezie, że dana osoba może być powiązana z ML/FT. Zewnętrzne zachowanie ujawnia więc nie tylko stosunek do relacji z instytucją, lecz także z zaoferowanym produktem i/lub usługą (jako przedmiotem zachowania). Stąd możliwe do wsparcia będzie zastosowanie rozwiązań określanych jako psychologia sprzedaży. Zrozumienie psychologicznych aspektów procesu obsługi klienta może wpłynąć na zwiększenie efektywności sprzedaży, ale także skonfrontować antysprzedażowe zachowanie klienta w kontekście opłacalności produktu. Może ponadto ujawnić ukryty cel aktywności klienta. Do możliwych zachowań ocenianych pod kątem możliwości zaangażowania klienta w proceder ML/FT zaliczymy:

- przekazywanie niespójnych informacji lub niechęć do udzielenia informacji oraz niechęć do wyjaśnienia szczegółów i błędów,
- nieuzasadnioną dysproporcję między stanowiskiem i/lub zawodem, profilem finansowym a transakcjami klienta,
- demonstrowanie innej postawy klienta niż ogólne modele postawy klienta,
- intensyfikację postawy negatywnej wobec sięgania po różną argumentację,
- stosowanie z różną intensywnością i efektem fałszywej identyfikacji,

N. Artienwicz, *Rachunkowość behawioralna jako interdyscyplinarny nurt rachunkowości i społecznych nauk o zachowaniu*, https://ztr.skwp.pl/api/files/view/148818.pdf, s. 7–23 [dostęp: 28 XI 2024].

- zdenerwowanie i niechęć do wyjaśniania lub kłamanie w przypadku rozpytania o doniesienia mediów, że klient jest powiązany ze znanymi organizacjami terrorystycznymi lub zaangażowany w działalność terrorystyczną,
- niechęć do podawania swojego nazwiska w zakresie formalizowania relacji z IO,
- pozorowanie negocjacji warunków umów i składanie „oferty" możliwości nieformalnego uzyskania określonych relacji (np. co do kwoty transakcji),
- stałe zmierzanie do przeprowadzenia transakcji w formie gotówkowej,
- kierowanie zapytań do przedstawiciela instytucji co do możliwości nierejestrowania przeprowadzenia transakcji,
- mylenie pojęć, obszarów geograficznych czy istotnych elementów przedmiotów umowy, kontraktu, transakcji,
- nieuzasadnioną aktywność klienta na koncie wobec dotychczasowej obserwowalnej statyki transakcyjnej,
- radykalną zmianę rodzajów zlecanych transakcji (np. uprawdopodabniających zachowania sprawcze),
- dokonywanie wpłat gotówkowych w przypadku prowadzenia działalności opartej głównie na transakcjach bezgotówkowych.

Innym tematem do rozważenia pozostaje sposób obsługi osób zajmujących eksponowane stanowiska polityczne (ang. *politically exposed persons*, PEP) i powiązanych z nimi podmiotów (gospodarczo, rodzinnie). W przypadku takich osób ich zachowanie można byłoby łączyć z kwestiami takimi jak: chęć uzyskania szybszych, wyższych czy długoterminowych korzyści. Z PEP wiąże się podwyższone ryzyko, dlatego IO musi stosować wobec nich wzmożone środki bezpieczeństwa finansowego. Pracownik IO powinien zwrócić uwagę na: wysokości kwot kontraktów wobec standardowych wynagrodzeń za dane postępowanie i uzyskany wynik, rodzaj powiązań z decydentem czy czas uzyskania promes, pozwoleń, zezwoleń (np. znaczne skrócenie czasu uzyskania tego rodzaju dokumentacji, a nawet brak zgodności z terminami administracyjnymi), ewentualnie miejsca potencjalnej działalności (zmiana statusu gruntów, budowa w okolicy parków narodowych, stref zielonych, obszarów typowanych pod rozbudowę infrastruktury logistycznej/drogowej itp.). Analiza tych informacji pozwala przygotować dla decydenta IO odpowiednie strategie, w tym te, jakie są sugerowane do zastosowania (lub pominięcia) przez członka zarządu instytucji. Bodźce mogą oddziaływać na PEP wobec potencjalnych zachowań korupcyjnych, zastraszania, dystrybucji środkami publicznymi, wpływaniem na transakcje finansowe czy uzgodnienia w ramach złożonych struktur korporacyjnych. Szczególnie oceniona powinna zostać sytuacja, gdy wobec specyficznie ukształtowanej struktury formalnej jedynym elementem brakującym pozostaje element finansowy. Nie chodzi jednak w tym przypadku

o sterowanie czy manipulację, lecz o uzyskanie wiedzy, czy tego typu struktura formalna nie powstała w wyniku powoływania się na wpływy, na utratę reputacji instytucji zaufania publicznego (która niejednokrotnie jest także instytucją finansową) czy uzyskania nieuprawnionej korzyści majątkowej (np. gdy stwierdzono, że przełożone dokumenty są niekompletne i/lub niewłaściwe, a jednak zostały zatwierdzone przez decydenta). Do oceny pozostaje więc zachowanie klienta mogące przejawiać się: zwiększoną pewnością siebie, powoływaniem się na znajomości, w tym w „kręgach władzy", sugestiami zadzwonienia do osób, z którymi wszystko zostało uzgodnione, zdenerwowaniem, gdy decydent wymaga dodatkowych wyjaśnień i/lub dokumentów, agresją klienta, który jest niezadowolony z postępowania pracownika IO i domaga się interwencji u jego przełożonego. Istotne jest pozyskanie wiedzy, na ile klient ma odpowiednie kompetencje czy wiedzę do zdobycia kontraktu, który chce sfinalizować w relacji z IO. Obserwując jego zachowanie, przedstawiciel IO powinien, na potrzeby oceny ryzyka związanego z taką osobą, stworzyć o niej raport informacyjny wynikający z zachowania. Można domniemywać, że w takim przypadku przedłożone dokumenty będą pozostawały w zgodności z ich formalnym wykorzystaniem, a jedynie po sposobie zachowania klienta będzie można ocenić, że ich wykorzystanie było wynikiem korupcji, czy też mają one posłużyć do pomnażania zysków szerszego kręgu osób (w tym np. PEP). Czynniki oddziałujące na zachowanie klienta mogą być związane z wyborem danej IO, możliwością manipulowania decyzjami osób zarządzających w IO w ramach sprawowanego nadzoru czy utrzymywania relacji towarzyskich z decydentami z IO. Dlatego też przedstawiciel tej instytucji z jednej strony będzie miał niewielkie pole do działania, a z drugiej, przy takim założeniu, może poszerzyć ocenę i skupić się na relacji i zachowaniu klienta w tej sytuacji, odmiennej od obsługi zwykłego klienta. W przypadku rozważania zachowania korupcyjnego zachowanie klienta będzie można oceniać na różnych etapach – dążenia do wręczenia korzyści lub oczekiwania korzyści za wręczone apanaże. W grę może także wchodzić zacieranie śladów przez PEP polegające na dezinformowaniu, w tym co do zamiarów, celu likwidacji konta, zmiany pełnomocników, wprowadzenia nowych przedstawicieli, beneficjentów rzeczywistych (np. pod pretekstem zmiany profilu działalności, wyjazdu do placówki dyplomatycznej, objęcia kierowniczego stanowiska w przedstawicielstwie w państwie trzecim UE itp.), oraz wykorzystywanie przepisów prawnych w celu nieujawniania i nieupubliczniania oświadczeń majątkowych (a w przypadku upublicznienia – nieujawniania w jego treści wszystkich istotnych informacji finansowych).

Problemem, z jakim może zmierzyć się przedstawiciel IO wobec zachowań klienta, zwłaszcza dotyczących chęci wsparcia działań terrorystycznych, będzie postawa akolity (kibica) terrorystycznego. Dotyczyć to będzie tych osób, które nie

chcą lub nie mogą być bezpośrednimi wykonawcami działań terrorystycznych, a starają się jednak, ze względu na swoje przekonania, postawę życiową, w jakiś sposób wspierać ten kierunek postępowania. Jedną z możliwości takiego wsparcia będzie udzielenie pomocy finansowej na realizację przedsięwzięć wykonawczych. Czynności te mogą być wykonywane zarówno z własnej inicjatywy, jak i w wyniku zewnętrznych determinantów (np. organizacji nielegalnych zbiórek pieniężnych). Tę postawę zresztą aktualnie umacnia aktywność terrorystów w mediach społecznościowych, kreujących postawy wspierające, którzy werbują osoby do udziału w aktywności terrorystycznej czy organizują zbiórki dla zwolenników ich ideologicznych celów realizowanych metodami terrorystycznymi. Warto także w tym zakresie zwrócić uwagę na to, czy z zachowania klienta można wywnioskować, że jest to jego pierwsze takie działanie, czy też jest ono powieleniem dotychczasowych. Warunkowanie instrumentalne to określony sposób uczenia się. Jeśli po zachowaniu następuje pozytywna konsekwencja (taka jak nagroda), istnieje większe prawdopodobieństwo, że zachowanie to powtórzy się w przyszłości[59]. Zwłaszcza że tą nagrodą może być ocena rzeczywista lub urojona[60] na podstawie zaistniałego aktu terrorystycznego. Należy tu podkreślić, że o ile członkowie grupy terrorystycznej w jakiś sposób są nastawieni także na zysk finansowy, o tyle w przypadku akolitów zysk ten nie ma wymiaru finansowego, a raczej dotyczy satysfakcji.

Artykuł 299 § 2 k.k. przewiduje karanie pracownika IO, który współdziała ze sprawcą procederu ML. Tym samym podejście behawioralne można zastosować również do oceny zachowań przedstawicieli IO[61]. W celu ujawnienia nieprawidłowości można wykorzystać UEBA[62] (ang. User and Entity Behavior Analytics), czyli

[59] A. Beltrani, *Understanding Behaviorism*, Palo Alto University, https://concept.paloaltou.edu/resources/business-of-practice-blog/understanding-behaviorsm [dostęp: 14 III 2024].

[60] Na przykład gdy osoba postronna przekazuje środki na rzecz określonego ugrupowania terrorystycznego, które w krótkim czasie od tego zdarzenia dokonuje zamachu terrorystycznego, to dana osoba wspierająca może zrozumieć to w ten sposób, że to ona swoim finansowym wsparciem bezpośrednio przyczyniła się do dokonania aktu terrorystycznego.

[61] W tym zakresie jako nietypowe zachowania wyróżnia się: zmiany w charakterystyce pracowników (np. wystawny styl życia, unikanie urlopów), zmiany w wynikach pracy pracownika lub agenta (np. sprzedawca sprzedający produkty za gotówkę odnotował znaczny lub nieoczekiwany wzrost wyników pracy), wszelkie transakcje z agentem, w ramach których tożsamość ostatecznego beneficjenta lub kontrahenta pozostaje nieujawniona, co jest sprzeczne ze zwykłą procedurą obowiązującą w danym rodzaju działalności. Zob. szerzej: *Types of Suspicious Activities or Transactions*, Financial Intelligence Unit Belize, 2016, https://fiubelize.org/types-of-suspicious-activities-or-transactions/ [dostęp: 18 XI 2024].

[62] User and Entity Behavior Analytics (UEBA) to „zaawansowane narzędzie analityczne, które monitoruje, analizuje i wykrywa anomalie w zachowaniach użytkowników oraz innych podmiotów (takich jak urządzenia, aplikacje i serwery) w sieci. UEBA wykorzystuje techniki uczenia maszynowego i analizy behawioralnej, aby identyfikować nietypowe wzorce aktywności, które mogą wskazywać

analizę zachowań użytkowników i podmiotów. Pracownicy IO pozostawiają w sieci cyfrowe ślady: uzyskują dostęp do określonych plików o konkretnych porach, rozpoczynają i kończą pracę zgodnie z rutyną, odwiedzają mniej więcej te same strony internetowe itp. W UEBA monitoruje się działania użytkowników i podmiotów oraz zbiera się o nich dane z logów systemowych, a do analizy ogromnych ilości danych wykorzystuje się zaawansowane metody oparte na uczeniu maszynowym. Dzięki zgromadzonym danym tworzy się punkt odniesienia dla zachowań użytkowników, znajduje się wzorce zachowań i odstępy między działaniami oraz ustala progi i odchylenia, w ramach których zachowanie jest uważane za normalne lub akceptowalne. Następnie tworzy się bazę wzorców zachowań użytkowników i porównuje je z zachowaniami pracowników o podobnym zakresie obowiązków w celu doprecyzowania i wykrycia ewentualnych odchyleń. W przypadku wykrycia anomalii system szacuje stopień odchylenia i poziom jego ryzyka oraz wysyła w czasie rzeczywistym alerty do pracowników ochrony. Każde rozwiązanie UEBA rejestruje unikalny zestaw danych zgodnie z przypadkami użycia, które obejmuje. Na przykład oprogramowanie UEBA może zbierać następujące informacje: godziny logowania i wylogowywania, prośby o dostęp do wrażliwych zasobów, odwiedzane strony internetowe, uruchomione aplikacje, podłączone urządzenia USB, dynamikę naciśnięć klawiszy. Od zebranych na tym etapie danych zależy skuteczność wszystkich pozostałych poziomów monitorowania zachowań[63]. W przypadku wykrywania zagrożeń wewnętrznych profile behawioralne służą do stworzenia zbioru negatywnych zachowań bazowych według przyjętych wzorców zachowań użytkowników (jako zbiorów uczących). Ta wartość bazowa pomaga kolejno systemowi wykryć nieprawidłowe działania użytkownika przy zastosowaniu metod uczenia maszynowego.

Biometria behawioralna jako sposób identyfikacji i weryfikacji klienta instytucji obowiązanej

Od jakiegoś już czasu biometria służy nie tylko do identyfikacji i weryfikacji tożsamości osoby (w tym klienta IO) na potrzeby utrzymywania relacji z instytucją, lecz także do wypełniania obowiązków związanych z systemem AML/CFT.

na zagrożenia bezpieczeństwa". Cyt. za: *Co to jest User and Entity Behavior Analytics?*, nFlo, https://nflo.pl/slownik/user-and-entity-behavior-analytics/ [dostęp: 12 X 2025].

[63] Zob. L. Pryimenko, *5 Levels of User Behavior Monitoring and Analytics*, Syteca, 13 XII 2023 r., https://www.ekransystem.com/en/blog/5-levels-user-behavior-monitoring [dostęp: 18 XI 2024]; A. Babko, *7 Best Practices for Building a Baseline of User Behavior in Organizations*, Syteca, 7 VII 2021 r., https://www.ekransystem.com/en/blog/best-practices-building-baseline-user-behavior [dostęp: 18 XI 2024].

Zastosowanie biometrii behawioralnej zwiększa liczbę czynników branych pod uwagę w algorytmach analitycznych (także w podzbiorach uczących) i przyspiesza w czasie rzeczywistym identyfikację odchyleń od ustalonych wzorców zachowań klienta dokonywaną przy wsparciu AI.

W biometrii wykorzystuje się dwa rodzaje danych: fizyczne i behawioralne. Pierwsze z nich są zbierane przez skanowanie cech fizycznych człowieka: linii papilarnych, twarzy, geometrii dłoni, tęczówki czy układu żył. Drugie opierają się na badaniu i ocenie zachowań, które są specyficzne dla danego użytkownika i trudne do naśladowania. W tym przypadku są badane nie tyle reakcje w kontaktach przedstawiciel IO – klient, ile relacje pomiędzy klientem a urządzeniem, z którego on korzysta (dotyczy to także wchodzenia w interakcje w serwisach internetowych). Biometria służy do uzyskania informacji o indywidualnych cechach klienta, weryfikacji jego aktywności i tego, czy źródłem tej aktywności jest osoba, której identyfikacyjne dane behawioralne zostały zebrane na wstępnym etapie nawiązywania kontaktu z IO. Dzięki niej klient nie musi stale potwierdzać swojej tożsamości, a IO ma dodatkowe narzędzia do monitoringu zachowań klienta pod kątem oceny ryzyka i stosowania środków bezpieczeństwa finansowego. Ciągłe monitorowanie zachowań klientów zwiększa możliwość weryfikacji ich tożsamości w dowolnym momencie aktywnej sesji, a nie tylko na etapie rejestracji czy logowania, a także możliwość wykrywania złośliwej aktywności i podejmowania na czas odpowiednich środków zaradczych[64].

W biometrii behawioralnej uwzględnia się unikalny sposób interakcji użytkownika z urządzeniem technicznym, którym posługuje się on do zarządzania swoimi środkami. Badanie nie dotyczy tego, co dokładnie klient robi w bankowości elektronicznej, tylko w jaki sposób. Interakcja klienta z aplikacjami i witrynami internetowymi tworzy wzorzec, a ostatecznie profil oczekiwanego zachowania. W tym przypadku bada się m.in. takie zachowania, jak: pora logowania, szybkość klikania myszką, tempo wprowadzania znaków i przewijania strony, kąt, pod jakim jest trzymany smartfon, wzorce przesuwania, wzór skrótów klawiaturowych/gestów, styl/szybkość chodzenia, styl pisania (szybkość, nacisk na klawiaturze, położenie palców). Jest to analiza behawioralna wykonywana za pomocą reguł prędkości (ang. *behavioral analysis via velocity rules*[65]). Analiza behawioralna prędkości

[64] *Behavioral Biometrics: What it is and How to Enable it*, Arkose Labs, https://www.arkoselabs.com/explained/behavioral-biometrics/ [dostęp: 12 III 2024].

[65] Kontrole prędkości to metoda zapobiegania oszustwom stosowana w przetwarzaniu płatności. Działają one przez monitorowanie częstotliwości i wzorca transakcji dokonywanych w określonym przedziale czasowym oraz wykrywanie nietypowych działań, takich jak duża liczba transakcji z jednego konta lub adresu IP. Oszuści często próbują wykorzystać skradzione dane karty tak szybko, jak to możliwe, zanim posiadacz karty to zauważy, a nagły wzrost liczby prób transakcji może być

klawiatury koncentruje się na interakcji użytkownika z klawiaturą, co znajduje zastosowanie w takich dziedzinach jak wykonawstwo muzyczne, biometria behawioralna i wydajność użytkownika[66].

Płatności ekspresowe działają na podstawie analizy częstotliwości, z jaką kupujący próbuje dokonać transakcji za pośrednictwem witryny IO, i wszczynają alarm w przypadku podejrzenia przestępstwa (np. w związku z wysoką częstotliwością nieudanych transakcji jednego klienta w ciągu dnia lub tygodnia). Są przy tym wykorzystywane następujące parametry: lokalizacje użytkowników i szczegóły adresów IP, urządzenia używane do łączenia i czas trwania, pory dnia, w których zazwyczaj odbywają się logowania, korzystanie z sieci VPN lub serwerów proxy, konfiguracja przeglądarki i systemu, typowe wzorce zakupów, zwykłe wartości transakcyjne, używane karty[67]. Wprowadzone techniki ocenne pozwalają bankom także zbierać dane z żyroskopu w telefonie i analizować typowe ułożenie ekranu. Weryfikacji behawioralnej podlega sposób używania klawiszy (alfanumeryczny, nawigacyjny, manipulacyjny). Jest możliwe także skorzystanie z danych rejestrujących interakcję użytkownika z aplikacją, które dostarczają informacji za pomocą map cieplnych, diagramów przepływu użytkownika, ścieżki nawigacji użytkownika. System rozpozna sposób użytkowania niezgodny z naszym profilem, np. zbyt wolne lub szybkie naciskanie klawiatury[68]. Biometria behawioralna jest budowana także

sygnałem ostrzegawczym o możliwym oszustwie. Kontrole prędkości mogą generować alerty lub blokować transakcje, jeśli przekroczą określone progi, co pomaga chronić firmy i klientów przed oszustwami. Zob. *What is a velocity check in payments? What businesses should know*, stripe, 30 VIII 2024 r., https://stripe.com/en-pl/resources/more/what-is-a-velocity-check-in-payments-what-businesses-should-know [dostęp: 12 X 2025].

[66] W tym zakresie jest możliwe zastosowanie m.in. reguły prędkości (lub filtr prędkości, ang. *velocity rule or velocity filter*) stanowiącej warunek oparty na logice, który ocenia częstotliwość występowania określonych zachowań w określonym czasie. Reguły prędkości są niezbędne, gdy statyczne, jednorazowe kontrole nie wystarczają. Wykrywają one subtelne i zależne od czasu wzorce, które ujawniają boty, próby wyłudzania danych uwierzytelniających i inne próby oszustw o dużej prędkości, zanim wyrządzą one szkody. Zob. *Velocity Checks*, https://seon.io/resources/dictionary/velocity-check/ [dostęp: 12 X 2025].

[67] *Behavioral Analysis*, https://seon.io/resources/dictionary/behavioral-analysis/ [dostęp: 27 XI 2024].

[68] Biometria behawioralna „umożliwia bieżącą analizę charakterystycznych wzorców zachowań użytkowników podczas korzystania z bankowości elektronicznej. Identyfikacja odstępstw od zarejestrowanego wcześniej profilu umożliwia wykrycie próby nieautoryzowanego dostępu i przejęcia konta. W ten sposób dostarcza bankom dodatkową warstwę zabezpieczeń, działającą równolegle do dotychczasowych metod uwierzytelnienia". Cyt. za: W. Macierzyński, M. Macierzyński, *Wykorzystanie biometrii behawioralnej w kontekście cyberbezpieczeństwa polskiego sektora bankowego (2019–2024)*, „Journal of Finance and Financial Law" 2025, t. 3, nr 47, s. 105. https://doi.org/10.18778/2391-6478.3.47.07. Ponadto „dzięki biometrii behawioralnej widać bowiem nie tylko, jakie litery są wprowadzane, ale również to, jak są wprowadzane. System widzi, że hasło co prawda się zgadza, ale nie zgadza się sposób jego wprowadzania. Bo ktoś inaczej trzyma telefon, wpisuje hasło lewą, a nie prawą

na tym, w jaki sposób klienci wchodzą w interakcje ze swoimi finansami, zarządzają transakcjami i kontami (cyfrowe portfele, platformy inwestycyjne)[69]. Podobne rozwiązania wykorzystuje się w relacji z chatbotami. W konsekwencji te działania mogą prowadzić do poszukiwania także określonych zależności pomiędzy aktywnością mózgu a zewnętrznym zachowaniem (neurobehawiorystyka[70]). Włączając analizy behawioralne do procesu analizy ryzyka (w tym w zakresie procesów wspomagania AI), można uzyskać natychmiastowy zwrot z inwestycji (ang. *return on investment*, ROI)[71], zmniejszenia strat związanych z oszustwami, obniżenia kosztów operacyjnych i poprawy zadowolenia klientów[72].

---

ręką lub robi za duże odstępy czasowe między wpisaniem kolejnej litery. Bo w innym rytmie wpisujemy hasło, które mamy w pamięci, a inaczej hasło, które spisujemy z kartki litera po literze". Cyt. za: W. Boczoń, *Naganowski: Nadchodzi biometria behawioralna*, prnews.pl, 16 I 2018 r., https://prnews.pl/naganowski-nadchodzi-biometria-behawioralna-432582 [dostęp: 12 X 2025].

[69] Tego typu rozwiązania są budowane także na emocjach, samodzielności w podejmowaniu decyzji, chęci osobistego realizowania się w zarządzaniu aktywami oraz sprawowaniu nad nimi kontroli. Zob. szerzej: S. Jahandari, J. Shaman, *Estimation in Networks With Spatiotemporally Correlated Noise*, „IEEE Transactions on Automatic Control" 2025, t. 70, nr 10, s. 6885–6892. https://doi.org/10.1109/TAC.2025.3565015; S. Jahandari, D. Materassi, *How Can We Be Robust Against Graph Uncertainties*, w: *2023 American Control Conference (ACC)*, s. 1946–1951. https://doi.org/10.23919/ACC55779.2023.10156615.

[70] Neurobehawiorystyka została zdefiniowana jako każda reakcja behawioralna wynikająca z przetwarzania ośrodkowego układu nerwowego. Neurobehawioralność jest uważana za podstawę wydajności w czynnościach dnia codziennego (ADL), m.in. odnosi się do poznawczych i percepcyjnych komponentów zachowania, w tym praksji, uwagi, pamięci, relacji przestrzennych, sekwencjonowania i rozwiązywania problemów. Zob. G. Gillen, K. Brockmann Rubio, *Treatment of Cognitive-Perceptual Deficits: A Function-Based Approach*, https://www.sciencedirect.com/sdfe/pdf/download/eid/3-s2.0-B9780323172813000277/first-page-pdf [dostęp: 12 X 2025]. Reakcje neurobehawioralne mogą zostać zaburzone przez czynniki środowiskowe, takie jak ekspozycja na neurotoksynę. Wyróżnik neurobehawioralny może wystąpić po latach u osoby dorosłej, mówi się wtedy o rozhamowaniu neurobehawioralnym (ang. *neurobehavior disinhibition*), które jest cechą utajoną, a wywodzącą się z szeregu wskaźników niedostatecznej kontroli behawioralnej, w tym z funkcji poznawczych wykonawczych, symptomatologii eksternalizacyjnej i dysregulacji emocjonalnej. Stąd istnieje możliwość identyfikacji indywidualnej klienta przez pogłębioną relację z IO w ramach stosowanych środków bezpieczeństwa finansowego (weryfikacji). Czynniki wpływu to niedostosowanie społeczne czy używanie narkotyków.

[71] Dzieli się on na: Trending ROI – są to wczesne, zorientowane na postęp wskaźniki, które sugerują, że inicjatywa AI przynosi wartość, nawet jeśli ta wartość nie przełożyła się jeszcze na przychody lub oszczędności, oraz Realized ROI – to mierzalny, zorientowany na wyniki wpływ inwestycji w AI. Zob. M. Bokich, *Measuring AI ROI: How to Build an AI Strategy That Captures Business Value*, Propeller, 8 V 2025 r., https://propeller.com/blog/measuring-ai-roi-how-to-build-an-ai-strategy-that-captures-business-value [dostęp: 12 X 2025].

[72] Z. Salman, *Behavioral Biometrics and Customer Identity Authentication*, Fico Blog, 19 I 2021 r., https://www.fico.com/blogs/behavioral-biometrics-and-customer-identity-authentication [dostęp: 14 III 2024].

Uwierzytelnienie oparte na aktywności użytkownika może być wykorzystane do oceny, czy ta aktywność nie pokrywa się ze znamionami bycia sprawcą w ramach procederu ML czy FT. Przez badanie poszczególnych przypadków i zachowań IO może wygenerować wzorce, jak zachowują się klienci mający cechy potencjalnych sprawców ML/FT. Instytucja obowiązana może podjąć działania mające na celu identyfikację indywidualną na podstawie oceny zachowania czy biometrii behawioralnej, również przy wykorzystaniu innych czynników kwantyfikujących przestępczo klienta wynikających z ogólnych czynników typujących zachowania przestępcze, indywidualnych związanych ze świadczeniem określonych usług (ogólnych ofert) IO, ale także na podstawie indywidualnych ofert kierowanych do określonego klienta, które w jego zachowaniu odbiegają od wypracowanego przez IO i przyjętego wzorca posługiwania się instrumentarium finansowym przynależnym do danej indywidualnej oferty.

Bankowość internetowa jest zatem zmianą nadzoru ze strony IO, z uwzględnieniem innych czynników zachowania niż te, które byłyby typowane w celu oceny zachowania następującego w wyniku fizycznej obecności klienta w siedzibie instytucji. Stosowane cechy behawioralne to: podpisy (kształt i dynamika), głos, dynamika pisania na klawiaturze, sposób chodzenia itp. W tym celu wykorzystuje się technologie informacyjno-komunikacyjne. Jednym ze sposobów weryfikacji użytkownika jest wykorzystanie do uwierzytelniania lub identyfikacji dynamiki naciśnięć klawiszy. Odnosi się ona do zautomatyzowanej metody identyfikacji lub potwierdzania tożsamości osoby na podstawie sposobu i rytmu pisania na klawiaturze. Wzorce pisania są pobierane głównie z klawiatur komputerowych, ale informacje można potencjalnie zbierać z dowolnego urządzenia wyposażonego w tradycyjne klawisze reagujące na dotyk (dla przykładu dotyczy to: telefonów komórkowych, urządzeń PDA, ang. *personal digital asisstant* – laptop, palmtop, netbook itp.). W przypadku dynamiki naciśnięć klawiszy szablon biometryczny używany do identyfikacji osoby opiera się na sposobie pisania, rytmie i szybkości pisania na klawiaturze. Pomiary stosowane do dynamiki naciśnięć klawiszy to czas przebywania i czas lotu. Czas przebywania to czas naciśnięcia klawisza. Z kolei czas lotu to czas pomiędzy zwolnieniem klawisza a naciśnięciem kolejnego klawisza. W przeciwieństwie do fizjologicznych czynników biometrycznych nie ma czegoś takiego jak absolutne dopasowanie do biometrii behawioralnej. Dlatego trudno dyskutować o wyjątkowości wzorca pisania. Musi być jasne, że przy dynamice naciśnięć klawiszy nie jest możliwe uzyskanie tak niskich współczynników FAR[73] i FRR[74], jak w przypadku

[73] FAR, czyli współczynnik fałszywej akceptacji, to prawdopodobieństwo, że system błędnie autoryzuje osobę nieuprawnioną, na skutek nieprawidłowego dopasowania danych biometrycznych do szablonu.

[74] FRR, czyli współczynnik fałszywych odrzuceń, to prawdopodobieństwo, że system błędnie odrzuci dostęp upoważnionej osobie z powodu niedopasowania danych biometrycznych do szablonu.

lepszych fizjologicznych czynników biometrycznych, w związku z czym nie może to być jedyny czynnik identyfikujący lub uwierzytelniający osobę[75].

Innym sposobem oceny klienta za pomocą biometrii behawioralnej jest biometria poznawcza[76]. Ma ona na celu uzyskanie informacji o użytkownikach przez generowanie bodźców zewnętrznych, takich jak wyświetlanie obrazów, w celu analizy reakcji układu nerwowego, czy też analizę miejsc często odwiedzanych przez użytkownika. Służy to stworzeniu unikalnej tożsamości, która zmienia się w zależności od zachowań użytkownika w danej lokalizacji. Monitorowanie wzorców aktywności użytkowników służy do realizacji celu, tj. do wykrycia nietypowych działań, które wskazują na większe ryzyko możliwości wystąpienia oszustwa (zarówno przez samego użytkownika, jak i osobę podszywającą się pod niego). Możliwe anomalie obejmują transakcje przeprowadzone z nietypowej lokalizacji, niezgodne z normalnym zachowaniem użytkownika związanym z lokalizacją, lub prośby o przesłanie dużych kwot pieniędzy na nieznane konto. Umożliwia to sygnalizowanie w czasie rzeczywistym oszukańczych działań i zapobieganie im[77]. Na te potrzeby mogą być budowane zbiory oparte na danych dotyczących sytuacji: jak określony klient zachowywał się do tej pory, gdy nie było podejrzeń co do jego zachowania, lub na podstawie wzorców ogólnych ujawnionych w różnych sprawach, w których określony rodzaj zachowania zidentyfikowano jako zachowanie sprawcy czynu ML/FT.

Biometria behawioralna może być także jednym z elementów tzw. uwierzytelniania wieloskładnikowego. To metoda uwierzytelniania elektronicznego, w której wymagane są co najmniej dwa czynniki (np. hasło i rozpoznawanie głosu), aby użytkownik mógł uzyskać dostęp do strony internetowej lub aplikacji.

Należy także zwrócić uwagę na kinestetykę. Każdy człowiek ma unikalny sposób ułożenia ciała, stylu chodzenia i trzymania urządzenia mobilnego. Na przykład

---

[75] *Biometric Solutions*, https://www.biometric-solutions.com/keystroke-dynamics.html [dostęp: 12 III 2024].

[76] „Cechy biometryczne mierzą odrębne cechy ludzi, zwykle (ale nie zawsze lub niecałkowicie) podyktowane ich genetyką. Opierają się na pomiarach i danych pochodzących z bezpośredniego pomiaru określonej części ciała człowieka. Odciski palców, tęczówka, twarz, zapach, siatkówka, ucho, układ naczyniowy, usta, geometria dłoni i DNA to przykłady kategorii biometrii fizjologicznej." Cyt. za: A. Grzybowski, *Sztuczna inteligencja w okulistyce 2023*, Przegląd Okulistyczny, https://przegladokulistyczny.pl/2024/09/13/sztuczna-inteligencja-w-okulistyce-2023-2 [dostęp: 15 X 2025]. W omawianym przypadku pozwala na identyfikację klienta i jego zachowania wobec sytuacji, gdy pomiędzy klientem a IO występuje urządzenie – przekaźnik sygnałów informacyjnych będący jednocześnie identyfikatorem klienta. Zob. szerzej: P. Magee, M. Ienca, N. Farahany, *Beyond neural data: Cognitive biometrics and mental Privacy*, „Neuron" 2024, t. 112, wyd. 18, s. 3017–3028. https://doi.org/10.1016/j.neuron.2024.09.004.

[77] *How is behavioral biometrics used for authentication?*, Incognia, https://www.incognia.com/the-authentication-reference/how-is-behavioral-biometrics-used-for-authentication [dostęp: 15 III 2024].

pozycja ciała może pomóc w zrozumieniu rozkładu masy ciała, a analiza chodu może dostarczyć informacji na temat szybkości poruszania się lub długości wykonywanych kroków. W tym celu jest możliwe skorzystanie z zapisów telewizji przemysłowej z kamer instalowanych w ramach systemów bezpieczeństwa IO.

Podsumowanie

Behawiorystyka jako metoda oparta na obserwacji zachowań może być stosowana do profilowania i typowania klientów IO jako potencjalnych sprawców i/lub podejrzanych w procederze prania pieniędzy czy finansowania terroryzmu. Instytucja może obserwować osobę, a z jej zachowania generować dane na potrzeby identyfikacji, weryfikacji i monitoringu klienta. Dane te są na tyle niepowtarzalne i indywidualne, że pozwalają identyfikować osobę zarówno w ramach fizycznej relacji z IO, jak i relacji online. Zachowanie jest jednak tylko jednym z wymiarów, na którego podstawie można oceniać postępowanie klienta. Innym jest wymiar psychologiczny – zrozumienie psychologii przestępców. Wiele osób zajmujących się ML nie uważa, że popełnia przestępstwo. Uzasadniają one swoje działania tym, że nie wyrządzają szkód społecznych, lub przedstawiają je jako konieczne w danych okolicznościach. Identyfikacja tych uzasadnień może pomóc odkryć wczesne oznaki przestępczego zamiaru.

Szybki rozwój biometrii behawioralnej w ostatnich latach, a jednocześnie uznanie, że ten sposób identyfikacji i weryfikacji jest bardziej skuteczny od dotychczasowych metod opartych na kodach, staje się przyszłością dla branż technologicznych mających zapewnić bezpieczeństwo zarówno IO, jak i klientom tych instytucji. Ważne w tym zakresie jest zapewnienie instytucji możliwości bieżącego zbierania tego rodzaju danych na potrzeby tworzenia zbiorów uczących i przetwarzania tej wiedzy przy wsparciu AI i uczenia maszynowego. Dotyczy to zwłaszcza instytucji, które obsługują dużą liczbę klientów i w związku z tym muszą analizować wiele danych. Informacje te mogą być wykorzystywane także np. do celów reklamowych, profilowania użytkowników czy analizy stron internetowych. Taka analiza jest przydatna, gdy IO na potrzeby identyfikacji rzeczywistych motywów wejścia klienta w relacje z nią korzysta z otwartych źródeł informacji. Behawioralne, biometryczne uwierzytelnienie jako część identyfikacji klienta może być pomocne w weryfikacji i monitoringu klienta w ramach prowadzenia w IO indywidualnej oceny ryzyka ML/FT. Ta tzw. mapa zachowania (ang. *behavior mapping*) pozwala na wysnuwanie wniosków co do zaangażowania klienta w proceder ML czy FT. Dzięki zastosowaniu podejścia behawioralnego oraz biometrii behawioralnej będzie można dokonywać segmentacji klientów i zbudować szerszy profil wychodzący poza relacje

gospodarcze z IO. Będzie on mógł dotyczyć także kwestii związanych z zachowaniem się i źródłami zachowania prezentowanego przez klienta. W konsekwencji IO może zbudować sobie na potrzeby oceny i analizy ryzyk ML/FT dodatkowy obszar i czynniki wartościujące zagrożenie, a tym samym kwalifikować zakres i intensywność zastosowania środków bezpieczeństwa finansowego.

Bazowanie jedynie na ocenie zachowania nie jest wystarczające do zakwalifikowania klienta jako osoby podejrzewanej o udział w procederze ML/FT. Należy w tym celu łączyć metody behawioralne z innymi metodami (np. psychologicznymi, z dziedziny neuronauk, ang. *neurosciences*[78]). Podobnie będzie można badać zachowania transakcyjne klienta nakierowane na wskazany cel przestępczy, ale także na potrzeby oceny, czy wystąpiło uzasadnione podejrzenie, że określona transakcja lub określone wartości majątkowe mogą mieć związek z ML lub FT (art. 86 ustawy o p.p.p.f.t./2018). Ponadto ze względu na rozwój techniki należałoby rozważyć, czy na potrzeby KYC i analizy ryzyka IO nie powinny uzyskać formalnych uprawnień do prowadzenia analityki behawioralnej[79]. Przy czym jedynie połączenie elementów psychologicznych i uzewnętrznionego zachowania stwarza pełny obraz behawioralny klienta na potrzeby nie tylko reaktywnego i proaktywnego wykrywania przestępstw ML/FT, lecz także pełnej analizy ryzyka w IO[80].

Przyjęte przez autora artykułu ogólne założenie badawcze uznające, że wobec potrzeby analizy ryzyka i typowania środków bezpieczeństwa finansowego w stanie określonego zagrożenia ML/FT wymagane jest od IO podjęcie działań w zakresie identyfikacji oraz rozpoznania zachowań klienckich z uwzględnieniem czynników behawioralnych – zostało zweryfikowane pozytywnie. Opierając się na przedstawionej diagnozie, należy uznać, że jednym z podstawowych elementów oceny KYC powinno być budowanie profilu behawioralnego klienta jako wyniku oceny jego zachowania będącego skutkiem jego charakteru, motywacji, zamiaru przestępczego, zdolności do identyfikacji zagrożenia oraz zachowania, które jest efektem impulsu zewnętrznego wobec niego (np. uleganie namowom do popełnienia przestępstwa,

[78] Por. P. Piotrowski, *Neurobiologiczne i psychospołeczne uwarunkowania racjonalności zachowań przestępczych – przegląd badań*, https://bazhum.muzhp.pl/media/texts/resocjalizacja-polska-polish-journal-of-social-rehabilitation/2011-tom-2/resocjalizacja_polska_polish_journal_of_social_rehabilitation-r2011-t2-s197-232.pdf [dostęp: 12 X 2025].

[79] Dla przykładu realizacji takich działań, jak: ocena sposobu typowania rodzaju i tworzenie konta, wypełnianie formularza umowy, wysyłanie formularza, dodawanie kolejnych usług do już posiadanego koszyka, zarządzanie koszykiem zakupowym, zapisywanie się do newslettera czy dokonywanie zakupu przedmiotu lub subskrypcji.

[80] M. Sotiriou, wpis na portalu LinkedIn, https://www.linkedin.com/posts/makis-sotiriou_the-psychology-of-money-launderers-a-missing-activity-7265318888265957377-izS3 [dostęp: 28 XI 2024].

szantażowi, konieczność spłaty zadłużenia w innej instytucji finansowej)[81]. Ocena behawioralna pozwala na uzyskanie wiedzy na temat motywów i celu działania klienta. Ma ona związek z jego osobowością, zmiennością jego zachowania, w tym zachowania pod wpływem osób trzecich.

Bibliografia

Al-Obaidi N.M.H., *Motives of the Terrorism Phenomenon Among Youth and the Role of Laws in Dealing with It*, „Akkad Journal of Law and Public Policy" 2021, nr 4, t. 1, s. 182–197. https://doi.org/10.55202/ajlpp.v1i4.85.

Bandura A., *Teoria społecznego uczenia się*, Warszawa 2007.

Bąbel P., *Terapia behawioralna zaburzeń rozwoju z perspektywy analizy zachowania*, „Psychologia Rozwojowa" 2011, t. 16, nr 3, s. 27–38. https://doi.org/10.4467/20843879PR.11.016.0189.

Di Wu, Xuhui Li, *A Systematic Literature Review of Financial Product Recommendation Systems*, „Information" 2025, nr 16. https://doi.org/10.3390/info16030196.

Falkowski A., Tyszka T., *Psychologia zachowań konsumenckich*, Gdańsk 2001.

Grzywacz J., *Segmentacja na rynku usług bankowych*, „Zeszyty Naukowe PWSZ w Płocku. Nauki Ekonomiczne" 2014, t. 20, s. 37–53.

Hara M., Kierzynka R., Kołodziejski P., *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, wyd. 1, stan prawny na 12 maja 2013 r.

Jahandari S., Materassi D., *How Can We Be Robust Against Graph Uncertainties*, w: *2023 American Control Conference (ACC)*, s. 1946–1951. https://doi.org/10.23919/ACC55779.2023.10156615.

Jahandari S., Shaman J., *Estimation in Networks With Spatiotemporally Correlated Noise*, „IEEE Transactions on Automatic Control" 2025, t. 70, nr 10, s. 6885–6892. https://doi.org/10.1109/TAC.2025.3565015.

Liedel K., *Profilowanie sprawców przestępstw terrorystycznych*, w: *Profilowanie kryminalne*, J. Konieczny, M. Szostak (red.) Warszawa 2011, s. 199.

[81] Zob. A. Tajak-Bobek, *Proces decyzyjny na przykładzie przestępczości przeciwko mieniu. Analiza jakościowa wywiadów pogłębionych*, „Ogrody Nauk i Sztuk" 2022, nr 12, t. 12. https://doi.org/10.15503/onis2022.29.46.

Macierzyński W., Macierzyński M., *Wykorzystanie biometrii behawioralnej w kontekście cyberbezpieczeństwa polskiego sektora bankowego (2019–2024)*, „Journal of Finance and Financial Law" 2025, t. 3, nr 47, s. 103–128. https://doi.org/10.18778/2391-6478.3.47.07.

Magee P., Ienca M., Farahany N., *Beyond neural data: Cognitive biometrics and mental Privacy*, „Neuron" 2024, t. 112, wyd. 18, s. 3017–3028. https://doi.org/10.1016/j.neuron.2024.09.004.

Mazurczak J., *Radykalizacja jako proces prowadzący do ekstremizmu i terroryzmu*, „Miscellanea Anthropologica et Sociologica" 2020, nr 21(2), s. 45–73.

Meloy J.R., Hoffmann J., Guldimann A., James D., *The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology*, „Behavioral Sciences and the Law" 2012, t. 30, nr 3, s. 256–279. https://doi.org/10.1002/bsl.999.

Merari A., *Academic research and government policy on terrorism*, „Terrorism and Political Violence" 1991, t. 3, s. 88–102.

Milanovic K., *Money Laundering and Other Forms of Financial Crime*, „Journal of Law and Politics" 2024, nr 5, s. 57–78. https://doi.org//10.69648/JJDU2862.

Olszak-Häußler K., *Rozumienie pojęcia „ślad" w ujęciu profilowania kryminalnego*, „Problemy Kryminalistyki" 2016, nr 291, s. 7–11.

Ranstrop M., *The Root Causes of Violent Extremism*, Brussels: European Commission, 2016, w: J. Mazurczak, *Radykalizacja jako proces prowadzący do ekstremizmu i terroryzmu*, „Miscellanea Anthropologica et Sociologica" 2020, nr 21(2), s. 45–73.

Slovic P., Weber E.U., *Perception of Risk Posed by Extreme Events*, w: *Regulation of Toxic Substances and Hazardous Waste*, wyd. 2, J.S. Applegate, J.G Laitos, J.M. Gaba, N.M. Sachs (red.), 2011.

Tajak-Bobek A., *Proces decyzyjny na przykładzie przestępczości przeciwko mieniu. Analiza jakościowa wywiadów pogłębionych*, „Ogrody Nauk i Sztuk" 2022, nr 12, t. 12. https://doi.org/10.15503/onis2022.29.46.

Załuski W., *Założenie deskryptywne ekonomicznej analizy prawa: człowiek jako homo oeconomicus*, w: *System prawny a porządek prawny*, O. Bogucki, S. Czepita (red.), Szczecin 2008.

Źródła internetowe

Artienwicz N., *Rachunkowość behawioralna jako interdyscyplinarny nurt rachunkowości i społecznych nauk o zachowaniu*, https://ztr.skwp.pl/api/files/view/148818.pdf [dostęp: 28 XI 2024].

Aziz Sbeih D., *Which Group has a More Sustainable Model of Terrorism*, https://washington-collegereview.files.wordpress.com/2019/09/sbeih_which-group-has-a-more-sustainable-model-of-terrorism-al-qaeda-or-isis.pdf [dostęp: 24 XI 2024].

Babko A., *7 Best Practices for Building a Baseline of User Behavior in Organizations*, Syteca, 7 VII 2021 r., https://www.ekransystem.com/en/blog/best-practices-building-baseline-user-behavior [dostęp: 18 XI 2024].

Behavioral Analysis, https://seon.io/resources/dictionary/behavioral-analysis/ [dostęp: 27 XI 2024].

Behavioral Biometrics: What it is and How to Enable it, Arkose Labs, https://www.arkoselabs.com/explained/behavioral-biometrics/ [dostęp: 12 III 2024].

Beltrani A., *Understanding Behaviorism*, Palo Alto University, https://concept.paloaltou.edu/resources/business-of-practice-blog/understanding-behaviorsm [dostęp: 14 III 2024].

Biometric Solutions, https://www.biometric-solutions.com/keystroke-dynamics.html [dostęp: 12 III 2024].

Bjelopera J.P., *The Islamic State's Acolytes and the Challenges They Pose to U.S. Law Enforcement*, https://sgp.fas.org/crs/terror/R44110.pdf [dostęp: 29 X 2025].

Boczoń W., *Naganowski: Nadchodzi biometria behawioralna*, prnews.pl, 16 I 2018 r., https://prnews.pl/naganowski-nadchodzi-biometria-behawioralna-432582 [dostęp: 12 X 2025].

Bokich M., *Measuring AI ROI: How to Build an AI Strategy That Captures Business Value*, Propeller, 8 V 2025 r., https://propeller.com/blog/measuring-ai-roi-how-to-build-an-ai-strategy-that-captures-business-value [dostęp: 12 X 2025].

Co to jest User and Entity Behavior Analytics?, nFlo, https://nflo.pl/slownik/user-and-entity-behavior-analytics/ [dostęp: 12 X 2025].

Comparison: Terrorist Financing, Money Laundering, and Financing the Proliferation of Weapons of Mass Destruction, Jersey Financial Services Commission, 14 IV 2022 r., https://www.jerseyfsc.org/industry/guidance-and-policy/comparison-terrorist-financing-money-laundering-and-financing-the-proliferation-of-weapons-of-mass-destruction/ [dostęp: 12 X 2025].

Counter Proliferation Financing. Guidance Notes, https://www.fsc.gi/uploads/CPF%20Guidance%20Notes.pdf [dostęp: 12 X 2025].

Czym jest PML i jakie zagrożenie stanowi dla AML? Metody działania umożliwiające przestępcom profesjonalne pranie pieniędzy oraz strategie w walce z PML, iaml, 6 X 2025 r., https://www.iaml.com.pl/wiedza/pml/ [dostęp: 12 X 2025].

Estevez E., *Behavioral Analytics: Meaning, Types, Criticism*, Investopedia, 29 I 2023 r., https://www.investopedia.com/terms/b/behavioral-analytics.asp [dostęp: 15 VII 2025].

Fernando S., *Behavioral Authentication: Improving Security and CX Without Compromise*, WSO2, 21 VII 2023 r., https://wso2.com/library/whitepapers/behavioral-authentication-improving-security-and-cx-without-compromise [dostęp: 28 XI 2024].

Francis R., He L., *Managing money laundering risks in digital payments. How digital payment providers can combat financial crime*, OliverWyman, https://www.oliverwyman.com/our-expertise/insights/2023/oct/anti-money-laundering-strategies-for-digital-payment-providers.html [dostęp: 15 VII 2025].

Gillen G., Brockmann Rubio K., *Treatment of Cognitive-Perceptual Deficits: A Function-Based Approach*, https://www.sciencedirect.com/sdfe/pdf/download/eid/3-s2.0-B9780323172813000277/first-page-pdf [dostęp: 12 X 2025].

Grzybowski A., *Sztuczna inteligencja w okulistyce 2023*, Przegląd Okulistyczny, https://przegladokulistyczny.pl/2024/09/13/sztuczna-inteligencja-w-okulistyce-2023-2 [dostęp: 15 X 2025].

Guidance for a Risk-Based Approach the Banking Sector, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf [dostęp: 20 I 2025].

How is behavioral biometrics used for authentication?, Incognia, https://www.incognia.com/the-authentication-reference/how-is-behavioral-biometrics-used-for-authentication [dostęp: 15 III 2024].

Major factors influencing consumer behavior, Clootrack, https://www.clootrack.com/knowledge-base/major-factors-influencing-consumer-behavior [dostęp: 18 XI 2024].

McKee A.J., *behaviorism | Definition*, Doc's CJ Glossary, https://docmckee.com/cj/docs-criminal-justice-glossary/behaviorism-definition/ [dostęp: 12 III 2024].

„*Muły finansowe*" *– ukryte zagrożenie w świecie bankowości online*, prnews.pl, 2 XII 2024 r., https://prnews.pl/muly-finansowe-ukryte-zagrozenie-w-swiecie-bankowosci-online-481242 [dostęp: 12 X 2025].

Piotrowski P., *Neurobiologiczne i psychospołeczne uwarunkowania racjonalności zachowań przestępczych – przegląd badań*, https://bazhum.muzhp.pl/media/texts/resocjalizacja-polska-polish-journal-of-social-rehabilitation/2011-tom-2/resocjalizacja_polska_polish_journal_of_social_rehabilitation-r2011-t2-s197-232.pdf [dostęp: 12 X 2025].

Pryimenko L., *5 Levels of User Behavior Monitoring and Analytics*, Syteca, 13 XII 2023 r., https://www.ekransystem.com/en/blog/5-levels-user-behavior-monitoring [dostęp: 18 XI 2024].

Risk assess your business for money laundering supervision, Gov.UK, 23 X 2014 r., https://www.gov.uk/guidance/money-laundering-regulations-risk-assessments [dostęp: 18 XI 2024].

Salman Z., *Behavioral Biometrics and Customer Identity Authentication*, Fico Blog, 19 I 2021 r., https://www.fico.com/blogs/behavioral-biometrics-and-customer-identity-authentication [dostęp: 14 III 2024].

Sekar H., *Recognize Your Customers: A Complete Guide on Customer Behavioral Cues and Building Customer Relationships*, 8 VII 2019 r., https://www.freshworks.com/freshdesk/customer-engagement/customer-behavioral-cues-building-customer-relationships-blog/ [dostęp: 12 III 2024].

Skrebneva O., Abramova A., *Why Behavioral Analytics is Key to Fraud Detection Today*, The Sumsuber, 14 V 2024 r., https://sumsub.com/blog/behavioral-analytics/ [dostęp: 24 XI 2024].

Sotiriou M., wpis na portalu LinkedIn, https://www.linkedin.com/posts/makis-sotiriou_the-psychology-of-money-launderers-a-missing-activity-7265318888265957377-izS3 [dostęp: 28 XI 2024].

The definition of unusual and unjustified transactions from the perspective of the risk of money laundering and terrorist financing, https://www.cnb.cz/export/sites/cnb/en/faq/.galleries/definition_of_unusual_and_unjustified_transactions_from_the_perspective_of_the_risk_of_money_laundering_and_terrorist_financing.pdf [dostęp: 14 III 2024].

Thomas D., *Profiling Part 1: The Psychology of Anti Money Launderers*, https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/governance-risk-compliance/white-paper/the-psychology-of-money-launderers.pdf [dostęp: 28 XI 2024].

Thomas D., *Profiling Part 2: The Psychology of Anti Money Launderers*, https://www.world-check.com/media/d/content_whitepaper_reference/WhitePaper_The_Psychology_Of_Anti_Money_Launderers.pdf [dostęp: 28 XI 2024].

Types of Suspicious Activities or Transactions, Financial Intelligence Unit Belize, 2016, https://fiubelize.org/types-of-suspicious-activities-or-transactions/ [dostęp: 18 XI 2024].

Velocity Checks, https://seon.io/resources/dictionary/velocity-check/ [dostęp: 12 X 2025].

What is a velocity check in payments? What businesses should know, stripe, 30 VIII 2024 r., https://stripe.com/en-pl/resources/more/what-is-a-velocity-check-in-payments-what-businesses-should-know [dostęp: 12 X 2025].

Wolniak R., Skotnicka-Zasadzień B., *Wybrane metody badania satysfakcji klienta i oceny dostawców w organizacjach*, https://www.researchgate.net/profile/Radoslaw-Wolniak/publication/41199963_Wybrane_metody_badania_satysfakcji_klienta_i_oceny_dostawcow_w_organizacjach/links/5ab63b2ba6fdcc46d3b45829/Wybrane-metody-badania-satysfakcji-klienta-i-oceny-dostawcow-w-organizacjach.pdf [dostęp: 18 XI 2024].

Rosyjskie źródła internetowe

Викторович К.А., Алексеевна Ш.О., *Террористический акт: особенности уголовноправовой и криминалистической характеристик*, „Союз Криминалистов и криминологов" (Wiktorowicz K.A., Aleksiejewna Sz.O., *Tierroristiczeskij akt: osobiennosti ugołownoprawowoj i kriminalisticzeskoj charaktieristik*, „Sojuz Kriminalistow i Kriminołogow") 2023, nr 1, https://crimeinfo.ru/wp-content/uploads/2023/08/2023-01.pdf, s. 98–104 [dostęp: 28 XI 2024].

Akty prawne

Rozporządzenie delegowane Komisji (UE) 2016/1675 z dnia 14 lipca 2016 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849 przez wskazanie państw trzecich wysokiego ryzyka mających strategiczne braki (Dz. Urz. UE L 254/1 z 5 VIII 2025 r.).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU z 2025 r. poz. 644).

Ustawa z dnia 25 czerwca 2009 r. o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw (DzU z 2009 r. nr 166 poz. 1317).

Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU z 2000 r. nr 116 poz. 1216).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2025 r. poz. 383).

Inne dokumenty

FATF REPORT. Professional Money Laundering, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf [dostęp: 12 X 2025].

Stanowisko Urzędu Komisji Nadzoru Finansowego dotyczące identyfikacji klienta instytucjonalnego i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideoweryfikacji, https://static.fintek.pl/uploads/2022/03/Stanowisko_UKNF_dot_wideoweryfikacji_klientow_instytucjonalnych.pdf [dostęp: 28 XI 2024].

Wytyczne na podstawie art. 17 i art. 18 ust. 4 dyrektywy (UE) 2015/849 dotyczących środków należytej staranności wobec klienta oraz czynników, które instytucje kredytowe i finansowe powinny uwzględnić podczas oceny ryzyka prania pieniędzy i finansowania terroryzmu związanego z indywidualnymi stosunkami gospodarczymi i transakcjami sporadycznymi („wytyczne w sprawie czynników ryzyka prania pieniędzy i finansowania terroryzmu") uchylające i zastępujące wytyczne JC/2017/37, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016937/Guidelines%20ML%20TF%20Risk%20Factors_PL.pdf [dostęp: 28 XI 2024].

Dr Maciej Aleksander Kędzierski

Doktor nauk prawnych, badacz niezależny, prelegent na studiach podyplomowych Akademii Leona Koźmińskiego w Warszawie, radca prawny, emerytowany funkcjonariusz Policji. Autor artykułów i monografii z zakresu przestępczości zorganizowanej, przeciwdziałania praniu pieniędzy, i finansowaniu terroryzmu, analityki finansowej, sankcji finansowych i działań *compliance*.