BIOMETRIA BEHAWIORALNA W BANKOWOŚCI

SYGN. PAB/WIB 4/2026

ISBN 978-83-979868-0-0

Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Warszawa, luty 2026

PROGRAM ANALITYCZNO BADAWCZY

O raporcie

Raport „Biometria behawioralna w bankowości" został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Autorzy

Raport przygotowany przez zespół w składzie:

Kierownik badań, redaktor raportu

dr hab. prof. UŚ Dariusz Szostek

Profesor Wydziału Prawa i Administracji Uniwersytetu Śląskiego, radca prawny. Dyrektor Centrum Naukowego Cyber Science. Specjalista z zakresu zarządzania cyberbezpieczeństwem, w tym wykładowca na studiach podyplomowych z zakresu cyberbezpieczeństwa: Akademia Koźmińskiego, Polska Akademia Nauk, Politechnika Śląska (Zarządzanie cyberbezpieczeństwem).

Specjalista z zakresu cyberbezpieczeństwa, paperless, kwalifikowanych usług zaufanych, tożsamości cyfrowej, cyfrowego obiegu dokumentów, algorytmizacji procesów, implementacji w organizacji algorytmów w tym AI w zgodności z wymogami cyberbezpieczeństwa, tokenizacji procesów w tym wykorzystanie blockchain oraz smart contract, implementacji prawa w algorytmy (inżynieria prawa), cywilista. Realizator projektów Horizon 2020 związanych z innowacjami w przemyśle – SHOP4CF i MAS4AI. Współtwórca m.in: koncepcji i legislacji eSądu w Lublinie – elektronicznego postępowania upominawczego; koncepcji i legislacji elektronicznego potwierdzenia odbioru, powszechnie stosowanego na Poczcie Polskiej (tablety na których potwierdza się odbiór pism); koncepcji i wdrożenia podpisu biometrycznego na tabletach min. biocertiX (wspólnego projektu Samsunga, Asseco i Xtension), koncepcji i wdrożenia oprogramowania Ius Case w wydawnictwie C.H. Beck. Założyciel i dyrektor Centrum naukowego – CYBER SCIENCE – Śląskiego Centrum Inżynierii Prawa, Technologii i Kompetencji Cyfrowych, zrzeszającego Uniwersytet Śląski, Politechnikę Śląską, Uniwersytet Ekonomiczny w Katowicach, Instytut EMAG sieci Łukasiewicza i NASK. Działacz w zakresie zarządzania Internetem, członek rady programowej IGF Poland Ekspert kadencji 2020–2024 Obserwatorium Parlamentu Europejskiego ds. Sztucznej inteligencji. Przewodniczący Zespołu ds. Cyberbezpieczeństwa Konferencji Rektorów Akademickich Szkół Polskich. W 2025 r. powołany przez wicepremiera K. Gawkowskiego na członka Rady Naukowej Instytutu Łączności. Autor licznych książek i opracowań w zakresie prawa nowych technologii – „Legal tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym". Inicjator serii metodyk związanych z technologią i prawem w wydawnictwie C.H. Beck. Członek licznych projektów w zakresie cyfryzacji. Współtwórca i partner w latach 2014–2024 kancelarii Szostek_Bar i Partnerzy, w latach 2017–2019 współpracownik PwC Legal, w latach 2019–2021 współpracownik Kancelarii Maruta-Wachta. Odpowiedzialny za szereg wdrożeń paperless w organizacjach (m.in. w bankach). Prezes Szostek_Digital spółka z o.o.

Eksperci raportu

dr inż. Rafał Tomasz Prabucki (prawnik)

Audytor wiodący ISO/IEC 27001, BCMS ISO 22301 oraz ISO/IEC 42001/2023. Posiadacz tytułu Certified in Cybersecurity (CC) wydanym przez (ISC). Doktor nauk prawnych i inżynier. COO w Szostek_Digital. Członek Społecznego Zespołu Ekspertów przez Prezesie Urzędu Ochrony Danych Osobowych. Adiunkt na Uniwersytecie Śląskim. Członek CYBER SCIENCE, SABI, ISSA Polska, ISACA. Założyciel LegalHackers Katowice. Asystent w zakończonych projektach dotyczących wykorzystania nowych technologii w przemyśle: MAS4AI na Uniwersytecie Śląskim i SHOP4CF na Uniwersytecie Opolskim. Alumn stypendiów w Polsce, Hiszpani i Niemczech. Prowadzący wykłady na Uczelniach w Polsce, Litwie i we Francji. Absolwent studiów podyplomowych Zarządzanie Cyberbezpieczeństwem.

dr inż. Adrian Radosław Kapczyński

Audytor wiodący ISO 27001, ISO 22301, CISA, CISM. Uczeń prof. Andrzeja Grzywaka. W ramach Politechniki Śląskiej audytor i konsultant z zakresu biometrii, lider zespołu badawczego. Członek zarządu sekcji Cyberbezpieczeństwa Polskiego Towarzystwa Informatycznego, Cybersecurity & Data Science Expert Wasko Group. Kierownik studiów podyplomowych Cyber Science „Zarządzanie cyberbezpieczeństwem" realizowanych na Politechnice Śląskiej ora koordynato podobszaru badawczego „cyberbezpieczeństwo". Członek IEEE, ACM, ISSA Polska. W ramach Politechniki Śląskiej pracownik naukowo dydaktyczny w Katedrze Zastosowań matematyki i metod Sztucznej Inteligencji.

dr inż. Jarosław Homa

Audytor wiodący ISO 27001, ISO 22301, Pełnomocnik Rektora ds. Cyberbezpieczeństwa, Wicedyrektor Centrum Cyberbezpieczeństwa Politechniki Śląskiej, Menedżer Zarządzania Cyberbezpieczeństwem, Architekt: IT/Cyberbezpieczeństwa. Wykładowca: Politechnika Śląska, Akademia WSB, PJATK. (zajęcia na: studiach MBA, podyplomowych CYBER SCIENCE, Jest ekspertem z zakresu sieci komputerowych i cyberbezpieczeństw i sztucznej inteligencji. Ekspert w systemach IT i OT, członek: PTI, ISSA Polska. Posiada certyfikaty PRINCE2, ITIL, AgilePM, Instruktor CISCO CCNA. Projektuje i wdraża rozwiązania z zakresu Cyberbezpieczeństwa w tym SOC w oparciu o wytyczne, NIST. w kontekście zamian i wymagań ustawy KSC i NIS-2.

Studia MBA w Wojskowej Akademii Technicznej – Zarządzanie Cyberbezpieczeństwem. Absolwent studiów doktoranckich na Politechnice Śląskiej w Gliwicach w dyscyplinie Informatyka techniczna i telekomunikacja – praca doktorska: Implementacja algorytmów synchronizacji urządzeń sieciowych SDN (ang. Software Defined Network, SDN) – uzyskała tytuł doktora inżyniera w dyscyplinie Informatyka techniczna i telekomunikacja. Absolwent studiów na Politechnice Śląskiej w Gliwicach, ukończył dwa kierunki studiów odpowiednio na kierunku Automatyka i Robotyka, gdzie uzyskała tytuł inżyniera w specjalności sterowniki i systemy sterowania, a następnie na kierunku Informatyka w specjalności bazy danych, sieci i systemy komputerowe, gdzie uzyskał tytuł magistra inżyniera z wynikiem bardzo dobrym. Jego zainteresowania naukowe obejmują: sieci komputerowe programowalne SDN, cyberbezpieczeństwo, systemy komputerowe.

O programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 r. jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wy korzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów – końcowych użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- Nowe technologie w sektorze bankowym, cyberbezpieczeństwo banków i systemy płatnicze
- Ekonomiczna analiza rozwoju sektora bankowego, stabilności banków, otoczenia makroekonomicznego
- Prawno-regulacyjne i legislacyjne uwarunkowania działalności sektora bankowego oraz wyzwania wynikające z orzecznictwa sądów krajowych i europejskich
- ESG i sustainable finance
- Prace analityczno-badawcze w zakresie poszczególnych obszarów funkcjonowania banków oraz w zakresie funkcjonowania wskaźników referencyjnych

Więcej na temat działalności programu na stronie www.pabwib.pl

Kontakt

dr Tomasz Pawlonka
Dyrektor Programu
m: 505 917 778
e: tpawlonka@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Agnieszka Wicha
m: 661 646 474
e: agnieszka.wicha@zbp.pl

Bartosz Przyborowski
m: 795 933 104
e: bartosz.przyborowski@zbp.pl

dr Radosław Ciukaj
m: 784 680 685
e: radoslaw.ciukaj@zbp.pl

Spis treści

Rozdział 1. Wprowadzenie

1.1. Cel i zakres pracy

Celem niniejszej pracy jest kompleksowa analiza biometrii behawioralnej jako narzędzia identyfikacji lub uwierzytelniania użytkowników w sektorze bankowym, ze szczególnym uwzględnieniem jej znaczenia dla cyberbezpieczeństwa oraz zgodności regulacyjnej w prawie Unii Europejskiej. **Praca zmierza do wykazania, że biometria behawioralna stanowi jakościowo odmienną kategorię mechanizmów uwierzytelniania, która nie powinna być oceniana wyłącznie przez pryzmat technologii biometrycznych sensu stricto, lecz jako element szerszej architektury zarządzania tożsamością cyfrową, bezpieczeństwa informacji oraz ochrony danych osobowych.**

Głównym celem badawczym jest zatem odpowiedź na pytanie, w jaki sposób biometria behawioralna może wspierać procesy uwierzytelniania klientów banków w warunkach rosnących zagrożeń cyberbezpieczeństwa, przy jednoczesnym poszanowaniu zasad ochrony danych osobowych, proporcjonalności oraz minimalizacji danych. W tym kontekście praca dąży do oceny, czy i w jakim zakresie rozwiązania oparte na analizie cech behawioralnych użytkownika mogą stanowić adekwatne uzupełnienie lub alternatywę dla tradycyjnych metod uwierzytelniania, w szczególności w środowisku bankowości cyfrowej i mobilnej.

W nawiązaniu do ww. celu badawczego, sformułowano następujące pytania badawcze:

- Jakie są kluczowe wyzwania uwierzytelniania klientów banku i jak są one osadzone w modelach zarządzania tożsamością?
- Czym biometria behawioralna różni się od tradycyjnych metod biometrycznych i jakie ma zalety oraz ograniczenia w usługach finansowych?
- Jakie cechy behawioralne są typowo wykorzystywane w bankowości i jak wygląda proces ich pozyskania oraz analizy?
- W jaki sposób biometria behawioralna wspiera wykrywanie nadużyć oraz ciągłą ocenę ryzyka w czasie rzeczywistym?
- Jakie są główne ryzyka etyczne i reputacyjne oraz jakie warunki są kluczowe przy użyciu danych behawioralnych?
- Które kierunki rozwoju zastosowań nowych technologii są najbardziej perspektywiczne dla banków?

Zakres pracy obejmuje analizę tożsamości cyfrowej jako konstrukcji prawno-technicznej, stanowiącej punkt wyjścia dla dalszych rozważań dotyczących mechanizmów identyfikacji i uwierzytelniania. W tym sensie biometria behawioralna nie jest rozpatrywana w oderwaniu od modeli zarządzania tożsamością, lecz w ścisłym powiązaniu z architekturą systemów IAM, CIAM, federacji tożsamości oraz normatywnym modelem tożsamości cyfrowej przyjętym w prawie Unii Europejskiej, w szczególności w regulacjach eIDAS i eIDAS2.

Praca koncentruje się na sektorze bankowym jako obszarze o podwyższonym poziomie ryzyka, wysokim stopniu regulacji oraz szczególnym znaczeniu zaufania publicznego. Analiza uwzględnia zarówno perspektywę technologiczną, związaną z mechanizmami gromadzenia i analizy danych behawioralnych, jak i perspektywę prawną, obejmującą ochronę danych osobowych, cyberbezpieczeństwo oraz wymogi wynikające z regulacji sektorowych, takich jak PSD2, DORA czy NIS2. W tym ujęciu biometria behawioralna traktowana jest jako narzędzie funkcjonujące na styku bezpieczeństwa operacyjnego, zarządzania ryzykiem oraz zgodności regulacyjnej.

Szczególne znaczenie w niniejszej pracy przypisano także perspektywie instytucjonalnej nadzoru nad rynkiem finansowym, w której analiza danych behawioralnych użytkowników systemów bankowych może pełnić funkcję narzędzia wspierającego realizację zadań w zakresie zapewnienia bezpieczeństwa, stabilności oraz odporności operacyjnej sektora bankowego. W tym ujęciu dane behawioralne nie są traktowane jako cel samodzielny ani jako środek identyfikacji osób fizycznych, lecz jako element umożliwiający wykrywanie anomalii, nadużyć oraz zagrożeń cyberbezpieczeństwa, które mogą wpływać na ciągłość działania instytucji finansowych i zaufanie do systemu finansowego jako całości. Tak rozumiane przetwarzanie danych wpisuje się w realizację interesu publicznego, polegającego na ochronie stabilności systemu finansowego oraz bezpieczeństwa obrotu, przy jednoczesnym uwzględnieniu zasad proporcjonalności, minimalizacji danych i ograniczenia

celu, charakterystycznych dla europejskiego modelu ochrony danych osobowych.

Zakres pracy nie obejmuje szczegółowej analizy algorytmów uczenia maszynowego ani implementacji technicznych konkretnych rozwiązań komercyjnych, o ile nie jest to niezbędne dla zrozumienia ich funkcji i implikacji prawnych. Celem nie jest również ocena efektywności poszczególnych produktów rynkowych, lecz identyfikacja kluczowych cech biometrii behawioralnej jako kategorii rozwiązań oraz ocena jej roli w architekturze bezpieczeństwa banków.

W konsekwencji niniejsza praca ma charakter interdyscyplinarny, łącząc analizę prawną, regulacyjną i organizacyjną z elementami wiedzy z zakresu cyberbezpieczeństwa i systemów informatycznych. Przyjęty zakres umożliwia sformułowanie wniosków istotnych zarówno dla praktyki bankowej, jak i dla dalszych badań nad rolą biometrii behawioralnej w systemach tożsamości cyfrowej oraz bezpieczeństwa usług finansowych.

1.2. Metody badawcze i źródła

Podstawową metodą badawczą jest analiza dogmatycznoprawna, obejmująca wykładnię przepisów prawa Unii Europejskiej oraz prawa krajowego regulujących zagadnienia ochrony danych osobowych, identyfikacji elektronicznej, cyberbezpieczeństwa oraz nadzoru nad rynkiem finansowym. Analizie poddano w szczególności regulacje RODO, eIDAS i eIDAS2, a także akty sektorowe istotne z perspektywy bankowości cyfrowej, takie jak PSD2, DORA oraz NIS2. Celem tej analizy jest identyfikacja ram prawnych, w których możliwe jest przetwarzanie danych behawioralnych w procesach uwierzytelniania oraz w działaniach nadzorczych, z uwzględnieniem zasad legalności, celowości, proporcjonalności i minimalizacji danych.

Uzupełniająco zastosowano metodę analizy funkcjonalnej, polegającą na badaniu relacji pomiędzy celami regulacyjnymi a rzeczywistym funkcjonowaniem mechanizmów technicznych wykorzystywanych w bankowości cyfrowej. Metoda ta pozwala na ocenę, w jaki sposób biometria behawioralna realizuje określone funkcje w architekturze bezpieczeństwa banków, w szczególności w zakresie wykrywania anomalii, zapobiegania nadużyciom oraz wzmacniania odporności operacyjnej. Analiza funkcjonalna umożliwia także ocenę adekwatności istniejących regulacji wobec dynamicznie rozwijających się technologii oraz identyfikację obszarów potencjalnych napięć pomiędzy wymogami bezpieczeństwa a ochroną prywatności.

W pracy wykorzystano również elementy analizy systemowej, ukierunkowanej na postrzeganie biometrii behawioralnej jako komponentu szerszego ekosystemu tożsamości cyfrowej, cyberbezpieczeństwa i nadzoru finansowego. Podejście to pozwala na uwzględnienie zależności pomiędzy różnymi poziomami regulacji (ogólnymi i sektorowymi), rolami poszczególnych podmiotów (banków, użytkowników, stron ufających, organów nadzorczych) oraz przepływami informacji w systemach bankowych. W tym ujęciu biometria behawioralna analizowana jest nie jako odizolowane narzędzie techniczne, lecz jako element infrastruktury zaufania, którego znaczenie ujawnia się w relacji pomiędzy bezpieczeństwem systemowym a ochroną praw jednostki.

Źródła wykorzystane w pracy obejmują w szczególności: akty prawa Unii Europejskiej i prawa krajowego, orzecznictwo sądów unijnych i krajowych w zakresie ochrony danych osobowych oraz identyfikacji elektronicznej, dokumenty instytucjonalne i wytyczne organów nadzorczych, a także literaturę naukową z zakresu prawa nowych technologii, cyberbezpieczeństwa i bankowości cyfrowej. Uzupełniająco wykorzystano opracowania techniczne oraz analizy branżowe, w zakresie niezbędnym do zrozumienia mechanizmów działania biometrii behawioralnej oraz jej roli w praktyce bankowej, bez wchodzenia w szczegółową analizę algorytmiczną.

Przyjęta metodologia badawcza umożliwia wielowymiarową ocenę biometrii behawioralnej, uwzględniającą zarówno jej potencjał w zakresie zwiększania bezpieczeństwa i odporności sektora bankowego, jak i ograniczenia wynikające z obowiązujących ram prawnych i zasad ochrony danych osobowych. Pozwala to na sformułowanie wniosków istotnych z perspektywy praktyki regulacyjnej, nadzorczej oraz dalszych badań nad rolą danych behawioralnych w systemach tożsamości cyfrowej.

1.3. Znaczenie tematu w kontekście sektora finansowego i cyberbezpieczeństwa

Znaczenie biometrii behawioralnej w sektorze finansowym należy rozpatrywać w szerszym kontekście transformacji cyfrowej bankowości oraz rosnącej skali i złożoności zagrożeń cyberbezpieczeństwa. Banki funkcjonują obecnie w środowisku, w którym większość kluczowych relacji z klientami realizowana jest za pośrednictwem kanałów cyfrowych, a dostęp do usług finansowych opiera się na zdalnych mechanizmach identyfikacji i uwierzytelniania. W takich warunkach bezpieczeństwo procesów uwierzytelniania przestaje być wyłącznie zagadnieniem technicznym, a staje się elementem determinującym stabilność operacyjną instytucji finansowych oraz zaufanie do systemu bankowego jako całości.

Sektor finansowy należy do obszarów szczególnie narażonych na zaawansowane formy cyberataków, w tym przejęcia kont, nadużycia transakcyjne oraz ataki socjotechniczne, które coraz częściej wykorzystują automatyzację i narzędzia sztucznej inteligencji. Jednocześnie klasyczne mechanizmy uwierzytelniania, oparte na modelu silnego uwierzytelnienia klienta (SCA), w tym na czynnikach wiedzy, posiadania i cechach klienta, pozostają skutecznym i powszechnie stosowanym fundamentem bezpieczeństwa w bankowości elektronicznej. Przykład Polski, utrzymującej wysoki poziom bezpieczeństwa systemów bankowych, potwierdza efektywność obecnego modelu regulacyjnego i operacyjnego. Równocześnie obserwowane zmiany regulacyjne, w tym projektowane rozwiązania w ramach PSR, zakładające większą elastyczność w konstrukcji mechanizmów SCA (np. możliwość wykorzystania dwóch elementów z tej samej kategorii), wskazują na ewolucję podejścia do bezpieczeństwa – od sztywnego modelu formalnego ku modelowi bardziej opartemu na analizie ryzyka. W tym kontekście biometria behawioralna nie powinna być postrzegana jako alternatywa dla klasycznych metod uwierzytelniania, lecz jako ich uzupełnienie – umożliwiające ciągłą ocenę ryzyka oraz wykrywanie anomalii w czasie rzeczywistym, szczególnie w sytuacjach, w których formalnie spełnione wymogi SCA nie eliminują ryzyka nadużycia.

Z perspektywy cyberbezpieczeństwa biometria behawioralna pełni funkcję warstwy detekcyjnej, która uzupełnia tradycyjne modele ochrony perymetrycznej i uwierzytelniania punktowego. Jej znaczenie polega nie tyle na jednoznacznej identyfikacji osoby fizycznej, ile na możliwości rozpoznawania nieprawidłowych wzorców zachowania wskazujących na potencjalne naruszenie bezpieczeństwa. Takie podejście wpisuje się w nowoczesne koncepcje zarządzania ryzykiem cybernetycznym, w których kluczowe znaczenie ma wczesne wykrywanie incydentów oraz zdolność organizacji do szybkiej reakcji i ograniczenia skutków zdarzeń.

Istotne znaczenie omawianego zagadnienia ujawnia się również na poziomie regulacyjnym i nadzorczym. Rosnąca liczba incydentów cyberbezpieczeństwa w sektorze finansowym oraz ich potencjalne skutki systemowe powodują, że organy nadzoru coraz większą wagę przywiązują do odporności operacyjnej instytucji finansowych oraz efektywności stosowanych przez nie mechanizmów bezpieczeństwa. W tym kontekście dane behawioralne mogą stanowić źródło informacji pozwalające na ocenę realnej skuteczności zabezpieczeń banków, wykraczającą poza formalne spełnienie wymogów regulacyjnych. Analiza takich danych umożliwia bowiem identyfikację zagrożeń, które nie są widoczne na poziomie dokumentacji czy deklaratywnych polityk bezpieczeństwa.

Znaczenie biometrii behawioralnej należy również rozpatrywać w kontekście obowiązujących i projektowanych ram prawnych Unii Europejskiej, które kładą coraz większy nacisk na zarządzanie ryzykiem, odporność operacyjną oraz cyberbezpieczeństwo sektorów krytycznych, w tym bankowości. Regulacje takie jak DORA czy NIS2 wzmacniają podejście oparte na ciągłym monitorowaniu ryzyka i zdolności do reagowania na incydenty, co sprzyja wykorzystaniu narzędzi analitycznych opartych na danych behawioralnych. Jednocześnie europejski model ochrony danych osobowych nakłada istotne ograniczenia na zakres i sposób przetwarzania takich danych, co czyni analizę ich zgodności z zasadami RODO kluczowym elementem dalszych rozważań.

Rozdział 2. Pojęcie i elementy tożsamości cyfrowej

2.1. Tożsamość a identyfikacja – uwagi wprowadzające

Rozważania nad tożsamością cyfrową należy rozpocząć od rozróżnienia pojęć tożsamości (ang. *identity*) oraz identyfikacji (ang. *identification*). W literaturze przedmiotu podkreśla się, że tożsamość odnosi się do zespołu cech konstytuujących jednostkę jako podmiot prawa, natomiast identyfikacja stanowi proces ustalania, czy dana osoba jest tym, za kogo się podaje, w określonym kontekście społecznym, prawnym lub technicznym[1].

W tym ujęciu identyfikacja nie tworzy tożsamości, lecz opiera się na jej reprezentacji, przyjmując postać zestawu informacji, cech lub atrybutów umożliwiających przypisanie działań, praw lub obowiązków określonemu podmiotowi. Rozróżnienie to zachowuje aktualność również w środowisku cyfrowym, w którym procesy identyfikacyjne są realizowane za pośrednictwem systemów informatycznych oraz zautomatyzowanych mechanizmów uwierzytelniania.

Jak zwraca uwagę S. Lips, N. Vinogradova, R. Krimmer i D. Draheim, wraz z rozwojem społeczeństwa cyfrowego pojęcie tożsamości uległo funkcjonalnemu przekształceniu – od kategorii ontologicznej ku kategorii operacyjnej, ściśle powiązanej z dostępem do usług, realizacją transakcji oraz wykonywaniem praw w przestrzeni cyfrowej[2].

2.2. Od tożsamości osobistej do tożsamości cyfrowej

W doktrynie P. Ruiu, S. Saiu oraz E. Grosso, wskazują na dwa podstawowe sposoby rozumienia pojęcia tożsamości cyfrowej. W znaczeniu szerokim termin ten bywa utożsamiany z wszelkimi formami obecności jednostki w środowisku sieciowym, w tym z tzw. tożsamościami wirtualnymi, pseudonimami lub profilami użytkowników. W znaczeniu węższym – istotnym z perspektywy prawa i regulacji – tożsamość cyfrowa definiowana jest jako zbiór informacji i zasobów przypisanych do konkretnego użytkownika w systemie informatycznym, które podlegają ochronie i są wykorzystywane w procesach uwierzytelniania oraz autoryzacji działań[3].

To drugie ujęcie dominuje w literaturze prawniczej oraz w dokumentach Unii Europejskiej, gdzie tożsamość cyfrowa postrzegana jest nie jako byt autonomiczny, lecz jako instrument umożliwiający bezpieczne uczestnictwo w obrocie cyfrowym. Kluczowe znaczenie ma tu powiązanie tożsamości cyfrowej z ochroną danych osobowych, prawem do prywatności oraz zasadą kontroli użytkownika nad informacjami dotyczącymi jego osoby, co znajduje odzwierciedlenie zarówno w RODO, jak i w regulacjach dotyczących identyfikacji elektronicznej[4].

2.3. Tożsamość cyfrowa jako konstrukcja prawno-techniczna w prawie UE

Na gruncie prawa Unii Europejskiej tożsamość cyfrowa nie jest pojęciem wyłącznie technicznym, lecz konstrukcją prawno-techniczną, której celem jest zapewnienie zaufania, bezpieczeństwa oraz skut-

1 P. Ruiu, S. Saiu, E. Grosso, „Digital Identity in the EU: Promoting eIDAS Solutions Based on Biometrics", Future Internet 16, 228, 2024; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, „Re-Shaping the EU Digital Identity Framework", Annual International Conference on Digital Government Research (dg.o 2022), June 15–17, 2022, Virtual Event, Republic of Korea. ACM, New York, NY, USA. https://doi.org/10.1145/3543434.3543652.

2 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

3 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

4 Tamże.

ków prawnych transakcji dokonywanych drogą elektroniczną[5]. Analiza regulacji rozporządzenia eIDAS[6] oraz propozycji europejskich ram tożsamości cyfrowej prowadzi do wniosku, że tożsamość cyfrowa opiera się na relacji pomiędzy[7]:

- użytkownikiem (podmiotem tożsamości),
- zestawem atrybutów identyfikacyjnych,
- mechanizmami uwierzytelniania,
- stronami ufającymi (*relying parties*),
- systemem prawnym nadającym tym relacjom określone skutki prawne

W tym sensie tożsamość cyfrowa nie stanowi prostego cyfrowego odpowiednika dokumentu tożsamości, lecz funkcjonuje jako dynamiczny model zarządzania informacją o podmiocie, dostosowany do potrzeb usług publicznych i prywatnych, w tym sektora finansowego.

Wskazuje na to między innymi definicja „identyfikacji elektronicznej" która zgodnie z art. 3 ust. 1 eIDAS oznacza proces używania danych identyfikujących osobę, w postaci elektronicznej, niepowtarzalnie reprezentującą osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą inną osobę fizyczną lub osobę prawną.

2.4. Elementy składowe tożsamości cyfrowej

Na podstawie analizy literatury oraz dokumentów regulacyjnych można wyróżnić następujące elementy tożsamości cyfrowej:

2.4.1. Podmiot tożsamości

Podmiotem tożsamości cyfrowej jest co do zasady osoba fizyczna lub osoba prawna, której dane osobowe oraz atrybuty identyfikacyjne są wykorzystywane w procesach identyfikacji elektronicznej oraz uwierzytelniania w systemach informatycznych. W literaturze przedmiotu podkreśla się, że tożsamość cyfrowa nie stanowi autonomicznego bytu oderwanego od jednostki, lecz jest funkcjonalną reprezentacją osoby fizycznej w środowisku cyfrowym, umożliwiającą jej uczestnictwo w obrocie prawnym i gospodarczym w formie elektronicznej[8].

Na gruncie prawa Unii Europejskiej podejście to znajduje potwierdzenie w regulacjach dotyczących identyfikacji elektronicznej, które konsekwentnie odwołują się do osoby fizycznej lub prawnej jako podstawowego punktu odniesienia dla mechanizmów identyfikacyjnych[9]. Tożsamość cyfrowa pełni w tym ujęciu rolę instrumentu prawnego, za pomocą

5 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt.; P. Ruiu, S. Saiu, E. Grosso, dz. cyt.; D. Szostek, R. Prabucki, M. Jakubik, Konsekwencje wprowadzenia w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (tzw. eIDAS 2) dokumentu 3.0 dla umów bankowych, Sygn. PAB/WIB 21/2024, 2024.

6 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transkacji elektronicznych na rynku wewnętrznym (z późniejszymi zmianami) L.257/73 oraz L 1183 z 2024 r.

7 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

8 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

9 Regulacje unijne definiują „identyfikację elektroniczną" jako proces używania danych w postaci elektronicznej, które niepowtarzalnie reprezentują osobę fizyczną lub prawną. Co więcej, „dane identyfikujące osobę" są zdefiniowane jako zestaw danych umożliwiający ustalenie tożsamości takiej osoby. Wymóg ten jest doprecyzowany w kontekście Europejskiego Portfela Tożsamości Cyfrowej (EUDI), który musi zapewniać, aby dane identyfikujące osobę niepowtarzalnie reprezentowały osobę fizyczną i były z nią powiązane. W przypadku osób fizycznych przepisy wprost wskazują na konieczność oparcia portfeli na oficjalnej tożsamości obywateli i rezydentów, co potwierdza, że punktem wyjścia jest zawsze konkretny podmiot prawa. Akty wykonawcze precyzują wręcz konkretne atrybuty (np. imię, nazwisko, data urodzenia), które muszą być wykorzystywane do identyfikacji osoby fizycznej. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (dalej eIDAS 2.0), motyw 19, art. 1; Rozporządzenie wykonawcze komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej, Załącznik.

którego możliwe jest przypisanie określonych działań, oświadczeń woli lub skutków prawnych konkretnej osobie, przy zachowaniu wymogów bezpieczeństwa, zaufania oraz ochrony danych osobowych[10]. Oznacza to, że tożsamość cyfrowa nie ma charakteru samoistnego, lecz zawsze pozostaje normatywnie i funkcjonalnie powiązana z podmiotem prawa, którego dotyczy[11].

Jednocześnie w doktrynie unijnej zwraca się uwagę, że relacja pomiędzy osobą fizyczną lub osobą prawną a jej tożsamością cyfrową ma charakter relacyjny i kontekstowy. Tożsamość ta ujawnia się bowiem wyłącznie w określonych interakcjach z tzw. stronami ufającymi, takimi jak organy administracji publicznej, instytucje finansowe czy dostawcy usług cyfrowych, ale także pomiędzy podmiotami prywatnymi. W zależności od celu danej interakcji wykorzystywane są różne atrybuty podmiotu, co prowadzi do odejścia od modelu pełnej identyfikacji na rzecz selektywnego i proporcjonalnego potwierdzania określonych cech osoby[12].

Takie ujęcie podmiotu tożsamości cyfrowej ma istotne znaczenie dla obrotu prawnego, w szczególności w sektorze bankowym i finansowym. Pozwala ono bowiem na zachowanie ciągłości pomiędzy tradycyjnym pojmowaniem podmiotowości prawnej a nowymi formami realizacji praw i obowiązków w środowisku cyfrowym, jednocześnie ograniczając ryzyko oderwania procesów identyfikacyjnych od osoby, której one dotyczą. W konsekwencji tożsamość cyfrową należy postrzegać nie jako substytut osoby fizycznej, lecz jako prawnie relewantny mechanizm jej identyfikacji, podporządkowany zasadom prawa Unii Europejskiej i ochrony praw podstawowych[13].

2.4.2. Atrybuty tożsamości

Atrybuty tożsamości cyfrowej stanowią informacje opisujące podmiot, które są wykorzystywane w procesach identyfikacji elektronicznej oraz uwierzytelniania w określonym kontekście prawnym lub funkcjonalnym. Mogą one mieć charakter identyfikacyjny (np. imię i nazwisko, numer identyfikacyjny), kwalifikacyjny (np. posiadanie określonych uprawnień, status prawny lub zawodowy) bądź sytuacyjny (np. status klienta, wiek, miejsce zamieszkania w określonym momencie). W literaturze przedmiotu podkreśla się, że tożsamość cyfrowa nie jest jednolitą i niezmienną całością, lecz składa się z wielu atrybutów, które mogą być wykorzystywane selektywnie, w zależności od celu i charakteru danej interakcji[14].

Takie ujęcie atrybutów prowadzi do odejścia od tradycyjnego modelu identyfikacji, opartego na ujawnianiu pełnego zestawu danych identyfikujących osobę, na rzecz modelu kontekstowego i proporcjonalnego. W nowym podejściu regulacyjnym Unii Europejskiej akcentuje się, że w wielu sytuacjach prawnych wystarczające jest potwierdzenie jedynie określonej cechy podmiotu (np. pełnoletniości, posiadania uprawnienia czy statusu klienta), bez konieczności ujawniania pełnej tożsamości osoby. Atrybuty pełnią w tym sensie rolę nośników prawnie relewantnych informacji, których zakres powinien być adekwatny do konkretnej czynności lub transakcji[15].

Koncepcja selektywnego ujawniania atrybutów znajduje swoje uzasadnienie zarówno w regulacjach dotyczących identyfikacji elektronicznej, jak i w zasadach ochrony danych osobowych. Ograniczenie zakresu ujawnianych informacji do minimum niezbędnego dla osiągnięcia danego celu sprzyja realizacji zasady proporcjonalności oraz minimalizacji danych, a jednocześnie wzmacnia zaufanie do mechanizmów identyfikacji elektronicznej. W tym ujęciu atrybuty nie są jedynie elementem technicznym, lecz centralnym komponentem normatywnego modelu tożsamości cyfrowej, który ma umożliwiać bezpiecz-

10 Tożsamość cyfrowa w ujęciu eIDAS służy jako narzędzie umożliwiające dostęp do usług publicznych i prywatnych oraz wywoływanie skutków prawnych – eIDAS 2.0, art. 1.

11 Tożsamość cyfrowa nie jest bytem niezależnym – jest funkcjonalnie i normatywnie „zakotwiczona" w podmiocie prawa.

12 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

13 Regulacje przewidują, że identyfikacja elektroniczna i poświadczenia atrybutów zapewniają sektorowi finansowemu elastyczność niezbędną do spełnienia wymogów dotyczących identyfikacji klienta (KYC), przeciwdziałania praniu pieniędzy (AML – w kontekście przyszłego Urzędu ds. Przeciwdziałania Praniu Pieniędzy) oraz ochrony inwestorów. Ponadto tożsamość cyfrowa jest kluczowa dla spełnienia wymogów silnego uwierzytelniania klienta (SCA) przy logowaniu do kont i inicjowaniu transakcji płatniczych (zgodnie z dyrektywą PSD2). Ostatecznie prywatne strony ufające działające w obszarze bankowości i usług finansowych, które są zobowiązane do stosowania silnego uwierzytelniania, będą musiały akceptować europejskie portfele tożsamości cyfroweje. ID. eIDAS 2.0 motyw 56, 62 oraz art. 1 ust. (art. 5f ust. 2).

14 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

15 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

ne i zgodne z prawem funkcjonowanie podmiotów w obrocie cyfrowym[16].

Z perspektywy prawa Unii Europejskiej istotne jest również to, że atrybuty tożsamości cyfrowej mogą pochodzić z różnych źródeł oraz podlegać różnym reżimom zaufania i odpowiedzialności. Ich znaczenie nie polega wyłącznie na treści informacyjnej, lecz także na gwarancjach co do ich autentyczności, aktualności i wiarygodności, które decydują o możliwości wywoływania skutków prawnych wobec stron trzecich. Niektóre z nich są powiązane z domniemaniami prawnymi, inne nie. W konsekwencji atrybuty należy postrzegać jako funkcjonalne ogniwo łączące osobę fizyczną, lub prawną, system identyfikacji elektronicznej oraz strony ufające, a nie jako prosty zbiór danych opisowych[17].

W prawie europejskim zdefiniowano pojęcie „atrybutu" w art. 3 ust. 43 eIDAS zgodnie z którym „atrybut oznacza cechę charakterystyczną, właściwość, prawo lub zezwolenie osoby fizycznej lub prawnej lub przedmiotu".

2.4.3. Mechanizmy uwierzytelniania

Mechanizmy uwierzytelniania stanowią funkcjonalny komponent tożsamości cyfrowej, służący potwierdzeniu, że podmiot korzystający z określonych atrybutów jest osobą, której te atrybuty dotyczą. W literaturze przedmiotu konsekwentnie podkreśla się, że uwierzytelnianie nie jest tożsame z tożsamością cyfrową, lecz pełni wobec niej rolę instrumentalną – umożliwia bowiem wiarygodne powiązanie działań podejmowanych w środowisku cyfrowym z konkretnym podmiotem prawa[18].

Na gruncie prawa Unii Europejskiej mechanizmy uwierzytelniania postrzegane są przede wszystkim przez pryzmat zapewnienia odpowiedniego poziomu zaufania i bezpieczeństwa w transakcjach elektronicznych. Ich znaczenie nie ogranicza się do aspektu technicznego, lecz ma charakter normatywny, ponieważ skuteczność uwierzytelnienia warunkuje możliwość wywoływania określonych skutków prawnych, w szczególności w relacjach pomiędzy użytkownikiem a stronami ufającymi. W tym sensie uwierzytelnianie stanowi element łączący warstwę technologiczną systemów identyfikacji elektronicznej z porządkiem prawnym, w którym oceniana jest ważność i wiarygodność czynności dokonywanych drogą elektroniczną[19]. Ma też różne poziomy. Inny poziom jest „zwykłego" uwierzytelnienia a inne przez kwalifikowane usługi zaufane, czy uwierzytelnienie atrybutów z źródła pierwotnego.

16 Rozporządzenie eIDAS 2.0 definiuje selektywne ujawnianie jako umożliwienie właścicielowi danych ujawniania jedynie niektórych części większego zbioru danych, tak aby podmiot otrzymujący (strona ufająca) uzyskał tylko informacje niezbędne do świadczenia usługi. Do tego Europejski portfel tożsamości cyfrowej musi technicznie umożliwiać selektywne ujawnianie atrybutów stronom ufającym. Funkcja ta ma na celu zwiększenie wygody użytkownika oraz ochrony danych osobowych. Przepisy wyraźnie stanowią, że przetwarzanie danych w ramach portfela musi być zgodne z zasadą minimalizacji danych wynikającą z RODO, a portfele mają zapewniać najwyższy poziom ochrony danych. Ograniczenie zakresu danych do minimum jest fundamentem modelu zaufania w nowym ekosystemie. Strony ufające (np. banki, urzędy) są zobowiązane do żądania jedynie takich danych, które są niezbędne i proporcjonalne do konkretnego celu/usługi. Akty wykonawcze wprowadzają mechanizm „wbudowanych reguł ujawniania" (*embedded disclosure policies*), które mają ostrzegać użytkownika, jeśli strona ufająca żąda danych wykraczających poza to, co jest konieczne lub do czego jest uprawniona – eIDAS 2.0, motyw 11, 30, 56, 59, art. 5a ust. 4; Rozporządzenie Wykonawcze Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli, motyw 7, 8, art. 3, pkt. 8 oraz 9 lit. a-b.

17 Różne są źródła oraz reżimy zaufania i odpowiedzialności. Kwalifikowane elektroniczne poświadczenia atrybutów (QEAA): Są wydawane przez kwalifikowanych dostawców usług zaufania. Podlegają one ścisłemu nadzorowi, a dostawca ponosi odpowiedzialność za ich prawidłowość. Muszą one spełniać rygorystyczne wymogi określone w załączniku V do rozporządzenia eIDAS 2.0. Elektroniczne poświadczenia atrybutów wydawane przez podmioty sektora publicznego (źródła autentyczne): Są to atrybuty wydawane przez podmiot odpowiedzialny za źródło autentyczne (np. rejestr państwowy) lub w jego imieniu. Choć nie muszą być wydawane przez kwalifikowanego dostawcę usług zaufania, prawo UE uznaje je za równoważne pod względem skutków prawnych, o ile spełniają określone wymogi techniczne i bezpieczeństwa. Niekwalifikowane poświadczenia: Mogą być wydawane przez innych dostawców usług zaufania i podlegają innym zasadom odpowiedzialności, często wynikającym z prawa krajowego lub sektorowego. eIDAS 2.0 art. 1 (lit. j, art. 45d); Rozporządzenie Wykonawcze komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu motyw 7, 14, art. 3, ust. 2.

18 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

19 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

Mechanizmy uwierzytelniania mogą opierać się na różnych kategoriach czynników, w tym na czynnikach opartych na wiedzy, posiadaniu lub cechach podmiotu. W kontekście rozwoju tożsamości cyfrowej szczególne znaczenie zyskują rozwiązania wykorzystujące cechy biometryczne, które – przy spełnieniu określonych wymogów prawnych i organizacyjnych – mogą zwiększać poziom bezpieczeństwa oraz ograniczać ryzyko nadużyć. Jednocześnie w literaturze zwraca się uwagę, że stosowanie zaawansowanych mechanizmów uwierzytelniania wiąże się z koniecznością zapewnienia zgodności z zasadami ochrony danych osobowych oraz poszanowania praw podstawowych, co wymaga odpowiedniego wyważenia interesów bezpieczeństwa i prywatności[20].

Istotnym elementem unijnego podejścia do uwierzytelniania jest także kontekstowość i proporcjonalność stosowanych mechanizmów. Oznacza to, że poziom i rodzaj uwierzytelnienia powinny być dostosowane do charakteru danej czynności lub transakcji, a nie prowadzić do nieuzasadnionego nadmiaru wymagań identyfikacyjnych. W tym ujęciu mechanizmy uwierzytelniania nie stanowią celu samego w sobie, lecz są narzędziem służącym realizacji zasady zaufania oraz zapewnieniu bezpieczeństwa obrotu elektronicznego, w tym w szczególności w sektorze finansowym.

2.4.4. Strony ufające i kontekst użycia

Tożsamość cyfrowa funkcjonuje zawsze w określonym kontekście relacyjnym, którego nieodłącznym elementem są tzw. strony ufające (*relying parties*). Pojęcie to odnosi się do podmiotów, które polegają na wynikach procesu identyfikacji elektronicznej oraz uwierzytelnienia w celu podjęcia określonych działań prawnych lub faktycznych wobec użytkownika, takich jak zawarcie umowy, udostępnienie usługi czy realizacja uprawnienia. W literaturze przedmiotu podkreśla się, że bez istnienia strony ufającej tożsamość cyfrowa pozostaje jedynie konstruktem technicznym, pozbawionym realnego znaczenia normatywnego[21].

Na gruncie prawa Unii Europejskiej strony ufające obejmują zarówno podmioty publiczne, jak i podmioty prywatne, w tym w szczególności instytucje finansowe, dostawców usług cyfrowych oraz inne podmioty uczestniczące w obrocie elektronicznym[22]. Ich rola polega nie tylko na technicznym „odbiorze" danych identyfikacyjnych lub atrybutów, lecz przede wszystkim na uznaniu skutków prawnych procesu identyfikacji, przeprowadzonego z wykorzystaniem określonych mechanizmów i środków bezpieczeństwa. Oznacza to, że zaufanie strony ufającej do systemu identyfikacji elektronicznej ma charakter prawnie relewantny i wpływa na ocenę ważności oraz skuteczności czynności dokonywanych drogą elektroniczną[23].

Istotnym elementem relacji pomiędzy użytkownikiem a stroną ufającą jest kontekst użycia tożsamości cyfrowej. Tożsamość nie jest bowiem wykorzystywana w sposób abstrakcyjny lub jednolity, lecz zawsze w odniesieniu do konkretnej sytuacji prawnej, celu transakcji oraz poziomu ryzyka związanego z daną czynnością. W zależności od kontekstu strona ufająca może wymagać potwierdzenia jedynie wybranych atrybutów podmiotu lub zastosowania określonego mechanizmu uwierzytelniania, co prowadzi do zróżnicowania praktyk identyfikacyjnych w różnych obszarach obrotu. Takie podejście znajduje uzasadnienie w unijnym modelu tożsamości cyfrowej, który

20 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

21 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

22 Pojęcie „strony ufającej" jest szerokie i obejmuje zarówno sektor publiczny, jak i prywatny. Zgodnie z art. 3 pkt 6 eIDAS 2.0 strona ufająca to „osoba fizyczna lub prawna, która polega na identyfikacji elektronicznej, europejskich portfelach tożsamości cyfrowej lub innym środku identyfikacji elektronicznej, lub na usłudze zaufania". Przepisy wprost wymieniają prywatne strony ufające, w tym instytucje finansowe (bankowość, usługi finansowe), jako podmioty, które będą zobowiązane do akceptowania portfeli tożsamości cyfrowej, jeśli prawo wymaga od nich silnego uwierzytelnienia klienta (np. w transporcie, energetyce, zdrowiu) – eIDAS 2.0 motyw 56, art. 1 (art. 3 pkt 6, art. 5f ust. 2).

23 Rola strony ufającej nie ogranicza się do pasywnego odbioru danych, ale wiąże się z aktywnym procesem wywołującym skutki prawne. Strony ufające polegają na portfelach i identyfikacji elektronicznej w celu spełnienia wymogów prawnych, takich jak „należyta staranność wobec klienta" (KYC) czy przeciwdziałanie praniu pieniędzy (AML) w sektorze bankowym. Użycie portfela zapewnia im „elastyczność oraz rozwiązania umożliwiające identyfikację klientów" zgodnie z prawem. Strony ufające są zobowiązane do rejestracji w państwie członkowskim oraz do przeprowadzania procedury uwierzytelniania i walidacji danych identyfikujących osobę. Muszą również potwierdzić swoją tożsamość wobec użytkownika (wzajemne uwierzytelnienie), co buduje zaufanie w relacji prawnej – eiDAS motyw 5, 62, art. 5b.

zakłada elastyczność oraz proporcjonalność stosowanych rozwiązań[24].

Relacyjny i kontekstowy charakter tożsamości cyfrowej ma szczególne znaczenie w sektorze bankowym i finansowym, gdzie strony ufające działają w warunkach podwyższonego ryzyka oraz podlegają szczególnym obowiązkom regulacyjnym. W tym obszarze tożsamość cyfrowa stanowi podstawę nie tylko dostępu do usług, lecz także realizacji wymogów związanych z bezpieczeństwem, przeciwdziałaniem nadużyciom oraz ochroną interesów klientów. Jednocześnie konieczność uwzględnienia kontekstu użycia sprzyja odejściu od jednolitego modelu identyfikacji na rzecz zróżnicowanych scenariuszy wykorzystania tożsamości cyfrowej, dostosowanych do charakteru relacji pomiędzy użytkownikiem a stroną ufającą[25].

W konsekwencji strony ufające oraz kontekst użycia należy uznać za integralny element konstrukcji tożsamości cyfrowej, decydujący o jej praktycznym znaczeniu i skuteczności w obrocie prawnym. To właśnie w tej relacji ujawnia się normatywny wymiar tożsamości cyfrowej, rozumianej nie jako zbiór danych czy mechanizm techniczny, lecz jako narzędzie umożliwiające realizację praw i obowiązków w środowisku cyfrowym, zgodnie z zasadami zaufania, bezpieczeństwa i proporcjonalności przyjętymi w prawie Unii Europejskiej[26].

2.5. Znaczenie tożsamości cyfrowej jako punktu wyjścia dla dalszych rozważań

Przedstawione ujęcie pojęcia i elementów tożsamości cyfrowej stanowi punkt wyjścia do dalszej analizy jej roli w sektorze bankowym. W szczególności umożliwia ono ocenę wpływu regulacji eIDAS oraz eIDAS2 na procesy identyfikacji klientów, zawierania umów oraz zapewnienia bezpieczeństwa obrotu elektronicznego. Zawiera też w sobie definicje prawne, w których znaczeniu będą używane w dalszej części raportu.

2.6. Modele zarządzania tożsamością cyfrową

2.6.1. Zarządzanie tożsamością cyfrową jako problem prawno-organizacyjny

Wyodrębnienie elementów tożsamości cyfrowej prowadzi do konieczności analizy sposobów ich zorganizowanego zarządzania w środowisku cyfrowym. Zarządzanie tożsamością cyfrową nie polega bowiem wyłącznie na technicznym przechowywaniu danych lub stosowaniu określonych mechanizmów uwierzytelniania, lecz obejmuje całokształt procesów związanych z tworzeniem, weryfikacją, utrzymywaniem, wykorzystywaniem oraz wygaszaniem tożsamości i powiązanych z nią atrybutów w relacjach pomiędzy użytkownikami a stronami ufającymi. W tym sensie zarządzanie tożsamością cyfrową stanowi problem o charakterze jednocześnie prawnym, organizacyjnym oraz technicznym, którego nie można sprowadzić wyłącznie do warstwy informatycznej[27].

24 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

25 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

26 Relacja między użytkownikiem a stroną ufającą jest ściśle regulowana przez zasady UE, co odróżnia ten model od czysto komercyjnych lub technicznych rozwiązań tożsamościowych. Strony ufające nie mogą żądać danych wykraczających poza to, co zadeklarowały i co jest niezbędne do świadczenia usługi. Mechanizm selektywnego ujawniania atrybutów technicznie wymusza realizację tej zasady prawnej. System opiera się na wzajemnym uwierzytelnianiu – nie tylko użytkownik identyfikuje się przed stroną ufającą, ale również strona ufająca musi potwierdzić swoją tożsamość wobec użytkownika, co buduje zaufanie do transakcji. Interakcje te muszą odbywać się przy zachowaniu wysokiego poziomu bezpieczeństwa, co jest gwarantowane przez procesy certyfikacji portfeli oraz systemy nadzoru. eIDAS 2.0 motyw 56, 59, art. 1 (art. 5b ust. 2, art. 5a ust. 5 lit b–d, art. 5c ust. 1, art. 9 ust. 6–7, art. 10).

27 Przepisy precyzują procedury wydawania danych identyfikujących osobę (PID) oraz elektronicznych poświadczeń atrybutów (EAA), w tym weryfikację tożsamości użytkownika przed ich wydaniem. Rozporządzenie wykonawcze komisji (UE) 2024/2977 art. 3 ust. 1-2 i 6-7. Portfel umożliwia bezpieczne żądanie, wybieranie, łączenie i udostępnianie danych stronom ufającym. System wymaga również rejestrowania transakcji, co jest elementem zarządzania użyciem. eIDAS art. 5a ust. 4 lit. a, Rozporządzenie Wykonawcze Komisji (UE) 2024/2979 art. 9 ust 1 oraz ust. 2. Dostawcy portfela i usług zaufania muszą zarządzać zmianami, w tym aktualizacjami zabezpieczeń i komponentów oprogramowania, aby utrzymać zgodność z wymogami certyfikacji. eIDAS 2.0, art. 8 ust 3 lit. f i g oraz ust. 4, załącznik 4 - 5. Działania w zakresie oceny dotyczące instancji portfela, pkt. 4. Istnieją szczegółowe procedury dotyczące unieważniania portfeli (np. w przypadku kradzieży lub śmierci użytkownika) oraz unieważniania danych identyfikujących osobę i poświadczeń atrybutów. Dostawcy muszą posiadać polityki unieważniania i udostępniać informacje o statusie ważności. W przypadku naruszenia bezpieczeństwa państwa członkowskie mają obo-

W artykule autorstwa Ruiu, Saiu oraz Grosso, podkreśla się, że tożsamość cyfrowa – rozumiana jako konstrukcja prawno-techniczna – wymaga istnienia określonego modelu zarządzania, który determinuje sposób sprawowania kontroli nad atrybutami, zakres odpowiedzialności poszczególnych podmiotów oraz możliwość wywoływania skutków prawnych wobec stron trzecich. Modele zarządzania tożsamością cyfrową określają w szczególności, kto jest uprawniony do tworzenia i modyfikowania tożsamości, w jakim zakresie użytkownik sprawuje nad nią kontrolę oraz w jaki sposób strony ufające mogą polegać na wynikach procesu identyfikacji i uwierzytelnienia[28].

Z perspektywy prawa Unii Europejskiej zarządzanie tożsamością cyfrową ma charakter funkcjonalny i relacyjny. Oznacza to, że znaczenie tożsamości cyfrowej ujawnia się dopiero w określonym kontekście użycia, w którym dochodzi do interakcji pomiędzy użytkownikiem a stroną ufającą. Modele zarządzania tożsamością nie są zatem neutralne normatywnie, ponieważ wpływają na zakres zaufania, jaki może zostać przypisany danym identyfikacyjnym, oraz na ocenę skutków prawnych czynności dokonywanych drogą elektroniczną. W tym ujęciu zarządzanie tożsamością cyfrową stanowi element infrastruktury zaufania, warunkującej funkcjonowanie usług publicznych i prywatnych w środowisku cyfrowym[29].

Istotnym zagadnieniem pozostaje także rozróżnienie pomiędzy zarządzaniem dostępem a zarządzaniem tożsamością. W praktyce organizacyjnej pojęcia te bywają utożsamiane, jednak z punktu widzenia analizy prawnej nie są one tożsame. Zarządzanie dostępem koncentruje się na przyznawaniu i egzekwowaniu uprawnień w ramach określonego systemu lub organizacji, natomiast zarządzanie tożsamością dotyczy szerszego zbioru procesów związanych z reprezentacją podmiotu, weryfikacją jego atrybutów oraz uznawaniem skutków prawnych identyfikacji przez inne podmioty. To rozróżnienie ma kluczowe znaczenie dla dalszej analizy poszczególnych modeli zarządzania tożsamością, w tym modeli scentralizowanych, federacyjnych oraz normatywnego modelu przyjętego w prawie Unii Europejskiej[30].

W konsekwencji zarządzanie tożsamością cyfrową należy postrzegać nie jako jednorodne rozwiązanie technologiczne, lecz jako zbiór odmiennych modeli, które różnią się stopniem centralizacji, rolą użytkownika, zakresem interoperacyjności oraz znaczeniem normatywnym. Analiza tych modeli pozwala uchwycić ewolucję podejścia do tożsamości cyfrowej – od rozwiązań wewnątrzorganizacyjnych, przez modele relacyjne, aż po systemowe ramy prawne o charakterze ponadnarodowym, czego przykładem są regulacje eIDAS i eIDAS2.

wiązek zawieszenia lub wycofania portfeli. eIDAS 2.0 art. 5a ust. 8–10, Rozporządzenie wykonawcze komisji (UE) 2024/2977 art. 5 ust 1–4, Rozporządzenie Wykonawcze komisji (UE) 2025/1569 art. 4 ust. 1; Rozporządzenie Wykonawcze komisji (UE) 2025/847 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do reagowania na naruszenia bezpieczeństwa europejskich portfeli tożsamości cyfrowej art. 3 ust. 4, art. 4 ust 1–2, art. 8 ust. 1.

28 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

29 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

30 Definicja „identyfikacji elektronicznej" wprost odnosi się do procesu używania danych, które niepowtarzalnie reprezentują osobę fizyczną lub prawną. System kładzie ogromny nacisk na weryfikację atrybutów (cech, właściwości, uprawnień) względem źródeł autentycznych (np. rejestrów państwowych). Tożsamość w tym ujęciu jest dynamicznym zbiorem potwierdzonych danych, a nie statycznym kontem. Przepisy definiuje skutki prawne identyfikacji i atrybutów (np. domniemanie integralności, równoważność z dokumentami papierowymi) oraz wymusza ich transgraniczne uznawanie. To potwierdza, że zarządzanie tożsamością w UE ma charakter normatywny (prawny), a nie tylko techniczny. eIDAS motyw 78, art. 1 ust. 3, art. 45b ust. 1-3, art 45c, 45e ust. 1. Choć termin „zarządzanie dostępem" nie jest definiowany wprost w słowniczku rozporządzenia, struktura przepisów wyraźnie oddziela dostarczanie tożsamości od jej wykorzystania do uzyskania dostępu. To strona ufająca (np. bank, urząd, platforma internetowa) polega na tożsamości cyfrowej w celu świadczenia usług. Tożsamość (portfel) jest tylko środkiem do celu, jakim jest dostęp do usługi. Strona ufająca musi zadeklarować „zamierzone użycie" portfela i wskazać, jakie dane są jej potrzebne do świadczenia konkretnej usługi. Oznacza to, że uprawnienia (dostęp) są nadawane w konkretnym kontekście przez stronę ufającą, na podstawie zweryfikowanej tożsamości dostarczonej przez portfel. Przepisy wyraźnie rozdzielają rolę dostawcy tożsamości (portfela/PID), od roli strony ufającej (konsumującej tożsamość dla celów dostępowych). eIDAS 2.0 motyw 5-7, art. 1 ust. 3 lit. c, ust 5 (art. 5a ust. 18 oraz art. 5b ust.2). Regulacje wskazują, że model UE (europejski portfel tożsamości cyfrowej) został zaprojektowany tak, aby użytkownik miał kontrolę nad swoją tożsamością niezależnie od systemów dostępowych poszczególnych usługodawców. Dostawcy tożsamości (portfela) nie powinni widzieć, do jakich usług użytkownik uzyskuje dostęp (rozdzielenie tożsamości od dostępu w celu ochrony prywatności). Jest to fundamentalna różnica w stosunku do modeli, w których dostawca tożsamości kontroluje również dostęp (częste w korporacyjnych systemach IAM). Tożsamość (portfel) ma umożliwiać dostęp do szerokiego wachlarza usług publicznych i prywatnych w całej Unii, co oznacza, że tożsamość jest jedna, a systemów zarządzania dostępem (u poszczególnych stron ufających) jest wiele. eIDAS 2.0 motyw 32, art. 1 ust. 5 (art. 5a ust. 5 lit b–d.).

2.6.2. Model scentralizowany – Identity and Access Management (IAM)

Model Identity and Access Management (IAM) stanowi jeden z najwcześniej rozwiniętych i najpowszechniej stosowanych sposobów organizacji procesów związanych z identyfikacją użytkowników w systemach informatycznych. Jego zasadniczym celem jest zarządzanie dostępem do zasobów organizacji, w szczególności poprzez tworzenie, utrzymywanie oraz egzekwowanie uprawnień przypisanych do określonych kont użytkowników. W tym ujęciu IAM pełni funkcję narzędzia organizacyjnego, służącego zapewnieniu bezpieczeństwa systemów oraz kontroli nad działaniami podejmowanymi w ich ramach[31].

Z perspektywy analizy prawnej należy jednak podkreślić, że model IAM nie zarządza tożsamością cyfrową w sensie normatywnym, lecz jedynie jej wewnętrzną reprezentacją, funkcjonującą w obrębie konkretnej organizacji lub systemu. Tożsamość użytkownika w modelu IAM ma charakter instrumentalny i techniczny – jest ona konstruowana na potrzeby kontroli dostępu i nie jest co do zasady przeznaczona do wywoływania skutków prawnych poza granicami danej struktury organizacyjnej. Taki sposób ujmowania tożsamości odpowiada podejściu, w którym identyfikacja użytkownika jest podporządkowana celom bezpieczeństwa i zarządzania zasobami, a nie realizacji praw i obowiązków w obrocie prawnym[32].

Charakterystyczną cechą modelu IAM jest jego wysoki stopień centralizacji. Organizacja pełni jednocześnie rolę podmiotu tworzącego tożsamość, zarządzającego atrybutami oraz decydującego o zakresie dostępu użytkownika do poszczególnych systemów. Użytkownik ma w tym modelu ograniczony wpływ na sposób wykorzystania przypisanych mu danych identyfikacyjnych, a relacja pomiędzy użytkownikiem a systemem ma charakter hierarchiczny. Taka konstrukcja sprzyja efektywnej kontroli wewnętrznej, jednak jednocześnie ogranicza możliwość przenoszenia tożsamości oraz jej elementów pomiędzy różnymi podmiotami lub kontekstami użycia[33].

W literaturze przedmiotu wskazuje się, że model IAM nie jest dostosowany do środowisk wielopodmiotowych i transgranicznych, w których tożsamość cyfrowa powinna być uznawana przez różne strony ufające. Brak interoperacyjności oraz silne powiązanie tożsamości z jedną organizacją powodują, że IAM nie odpowiada na potrzeby współczesnego obrotu cyfrowego, w szczególności w zakresie usług publicznych i finansowych, gdzie kluczowe znaczenie ma możliwość polegania na identyfikacji dokonanej przez inny podmiot[34].

Z punktu widzenia prawa Unii Europejskiej model IAM należy zatem postrzegać jako rozwiązanie o ograniczonym znaczeniu normatywnym, które może skutecznie funkcjonować w ramach struktur wewnętrznych organizacji, lecz nie stanowi samodzielnego modelu zarządzania tożsamością cyfrową w rozumieniu regulacyjnym. Jego rola sprowadza się przede wszystkim do zapewnienia bezpieczeństwa i porządku organizacyjnego, a nie do budowania infrastruktury zaufania pomiędzy niezależnymi podmiotami. Ta cecha odróżnia IAM od bardziej zaawansowanych modeli, takich jak federacja tożsamości czy rozwiązania przyjęte w ramach eIDAS, które zakładają relacyjny i ponadorganizacyjny charakter tożsamości cyfrowej[35].

31 Zob. M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, Biometria w bankowości elektronicznej – Rynek, technologia, klient, SYGN. WIB PAB 8/2022, 2022.

32 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

33 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., P. Ruiu, S. Saiu, E. Grosso, dz. cyt., S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

34 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

35 Rozporządzenie definiuje „system identyfikacji elektronicznej" jako system, w ramach którego wydaje się środki identyfikacji osobom fizycznym lub prawnym, oraz „usługi zaufania". Systemy IAM, służące do zarządzania uprawnieniami wewnątrz organizacji, nie mieszczą się w tych definicjach regulacyjnych, chyba że zostaną oficjalnie notyfikowane jako system identyfikacji elektronicznej przez państwo członkowskie, co jest procedurą zastrzeżoną dla rozwiązań o znaczeniu publicznym lub szerokim zastosowaniu rynkowym. Regulacje eIDAS 2.0 skupiają się na interakcjach „na zewnątrz" – między użytkownikiem a stroną ufającą (usługodawcą). Sposób, w jaki strona ufająca zarządza tymi uprawnieniami wewnątrz swojej struktury (czyli domena IAM), pozostaje poza bezpośrednim zakresem regulacji tożsamości, podlegając raczej ogólnym przepisom o cyberbezpieczeństwie (np. NIS2) i ochronie danych (RODO. Model UE opiera się na „zaufanych listach", kwalifikowanych dostawcach usług zaufania oraz organach nadzoru, które gwarantują, że dany atrybut lub podpis jest ważny w całej Unii. IAM nie tworzy takiego łańcucha zaufania dla podmiotów zewnętrznych; służy jedynie ochronie zasobów danej organizacji. Regulacje kładą nacisk na wzajemne uwierzytelnianie (mutual authentication) między niezależnymi stronami – użytkownikiem portfela a stroną ufającą. IAM z definicji działa w obrębie jednej domeny zaufania (organizacji), co potwierdza tezę o jego odmienności od modelu eIDAS. European Digital Identity Architecture and Reference Framework – Outline –, 2012.

2.7. Model konsumencki – Customer Identity and Access Management (CIAM)

Model Customer Identity and Access Management (CIAM) stanowi rozwinięcie klasycznych rozwiązań IAM, dostosowane do obsługi relacji pomiędzy organizacją a klientami lub użytkownikami zewnętrznymi. Jego zasadniczym celem jest umożliwienie bezpiecznego dostępu do usług cyfrowych oferowanych na szeroką skalę, przy jednoczesnym zarządzaniu kontami użytkowników, procesami rejestracji, logowania oraz utrzymania profili klientów. W przeciwieństwie do IAM, który koncentruje się na relacjach wewnątrzorganizacyjnych, CIAM funkcjonuje w kontekście masowego i dynamicznego obrotu usługowego, w którym tożsamość użytkownika pełni rolę punktu dostępu do usług, a nie jedynie narzędzia kontroli wewnętrznej[36].

Z perspektywy analizy prawnej CIAM nie stanowi jednak autonomicznego modelu tożsamości cyfrowej w sensie normatywnym, lecz pozostaje rozwiązaniem organizacyjno-technologicznym, podporządkowanym celom konkretnego dostawcy usług. Tożsamość użytkownika w modelu CIAM jest tworzona i zarządzana przez usługodawcę, który decyduje o zakresie gromadzonych atrybutów, sposobie ich wykorzystania oraz zasadach dostępu do usług. Oznacza to, że podobnie jak w modelu IAM, tożsamość ma charakter pochodny i instrumentalny, a jej znaczenie prawne ogranicza się zasadniczo do relacji pomiędzy użytkownikiem a danym podmiotem[37].

Istotną cechą modelu CIAM jest jego rozszerzenie o funkcje związane z zarządzaniem danymi klientów, w tym zgodami, preferencjami oraz historią interakcji. W praktyce prowadzi to do silnego powiązania mechanizmów identyfikacji i uwierzytelniania z procesami marketingowymi, personalizacją usług oraz analizą zachowań użytkowników. W literaturze zwraca się uwagę, że takie podejście sprzyja efektywności biznesowej, lecz jednocześnie może prowadzić do zacierania granicy pomiędzy identyfikacją a profilowaniem, co rodzi istotne wyzwania z punktu widzenia ochrony danych osobowych oraz autonomii informacyjnej użytkownika[38].

Model CIAM charakteryzuje się również asymetrią kontroli nad tożsamością cyfrową. Chociaż użytkownik posiada możliwość zakładania i zarządzania kontem, rzeczywista kontrola nad atrybutami oraz ich dalszym wykorzystaniem pozostaje po stronie dostawcy usługi. Tożsamość użytkownika jest zatem ściśle związana z konkretną platformą lub ekosystemem usługowym i co do zasady nie podlega przenoszeniu pomiędzy różnymi podmiotami. Brak interoperacyjności oraz uznawalności tożsamości poza danym środowiskiem powoduje, że CIAM nie odpowiada na potrzeby transgranicznego obrotu prawnego ani nie zapewnia jednolitych skutków prawnych wobec stron trzecich, co odróżnia go od modeli relacyjnych i regulacyjnych[39].

W praktyce sektora bankowego rozwiązania CIAM są powszechnie wykorzystywane w bankowości elektronicznej i mobilnej jako podstawowy mechanizm obsługi klientów indywidualnych, w szczególności na etapie dostępu do usług, autoryzacji operacji oraz personalizacji interfejsów użytkownika. Analizy instytucjonalne wskazują jednak, że mimo rosnącej dojrzałości tych rozwiązań pozostają one ściśle powiązane z infrastrukturą konkretnego banku i nie funkcjonują jako element ponadinstytucjonalnych ram zaufania. W konsekwencji CIAM należy postrzegać jako model przejściowy pomiędzy wewnętrznym zarządzaniem dostępem a bardziej zaawansowanymi formami zarządzania tożsamością cyfrową, które zakładają relacyjność, interoperacyjność oraz uznawalność skutków prawnych w szerszym kontekście regulacyjnym[40].

Pobrane: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline; eIDAS motyw 1, art. 1, ust. 1, ust. 3, lit. a oraz c–d, ust. 4 (art. 5b), ust. 7–8, ust. 15 (art. 14 i art. 16).

36 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe; P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

37 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

38 Tamże.

39 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt. całe.

40 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe.

2.8. Federacja tożsamości jako model relacyjny

Model federacji tożsamości stanowi istotny etap ewolucji zarządzania tożsamością cyfrową, polegający na rozdzieleniu ról pomiędzy podmiotem identyfikującym a podmiotem świadczącym usługę oraz na uznawaniu wyników identyfikacji dokonywanej przez inny podmiot. W przeciwieństwie do modeli scentralizowanych, takich jak IAM i CIAM, federacja tożsamości nie opiera się na jednym, zamkniętym systemie zarządzania tożsamością, lecz na relacji zaufania pomiędzy niezależnymi uczestnikami, w ramach której tożsamość użytkownika może być wykorzystywana w wielu kontekstach usługowych[41].

Z perspektywy analizy prawnej kluczową cechą federacji tożsamości jest jej relacyjny charakter. Tożsamość cyfrowa nie jest w tym modelu „posiadana" przez jeden podmiot, lecz funkcjonuje jako rezultat współdziałania co najmniej trzech ról: użytkownika, dostawcy tożsamości oraz strony ufającej. Oznacza to przesunięcie akcentu z kontroli nad tożsamością na uznawalność procesu identyfikacji, który musi spełniać określone kryteria zaufania, bezpieczeństwa oraz wiarygodności. W literaturze podkreśla się, że federacja tożsamości redefiniuje sposób postrzegania tożsamości cyfrowej, traktując ją jako instrument relacyjny, a nie wyłącznie wewnętrzny zasób organizacji[42].

Istotnym elementem modelu federacyjnego jest interoperacyjność, rozumiana jako zdolność różnych systemów i podmiotów do wzajemnego uznawania tożsamości oraz powiązanych z nią atrybutów. Interoperacyjność ta nie ma wyłącznie charakteru technicznego, lecz obejmuje również wymiar prawny i organizacyjny, w tym ustalenie zasad odpowiedzialności, zakresu zaufania oraz skutków prawnych identyfikacji. W tym sensie federacja tożsamości stanowi próbę odpowiedzi na ograniczenia modeli IAM i CIAM, które nie zapewniają przenoszalności ani uznawalności tożsamości poza granicami pojedynczej organizacji[43].

Nowe ramy prawne i towarzyszące im rozporządzenia wykonawcze wskazują, że model federacyjny wiąże się z określonymi ryzykami, w szczególności z koncentracją zaufania po stronie wybranych dostawców tożsamości oraz złożonością relacji pomiędzy uczestnikami federacji. Skuteczność tego modelu zależy bowiem od istnienia wspólnych ram zaufania, które określają minimalne wymagania w zakresie bezpieczeństwa, ochrony danych oraz procedur identyfikacyjnych. Brak takich ram może prowadzić do fragmentaryzacji systemów oraz osłabienia zaufania stron ufających do wyników procesu identyfikacji[44].

W kontekście sektora bankowego federacja tożsamości znajduje zastosowanie przede wszystkim w scenariuszach wymagających uznania tożsamości potwierdzonej przez inny podmiot, w tym w relacjach pomiędzy bankami, administracją publiczną a dostawcami usług cyfrowych. Analizy praktyki instytucjonalnej wskazują jednak, że bez jednoznacznych i powszechnie akceptowanych ram regulacyjnych federacja tożsamości pozostaje rozwiązaniem częściowym, którego wdrożenie i skuteczność zależą od indywidualnych porozumień oraz poziomu zaufania pomiędzy uczestnikami[45].

41 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

42 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

43 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt. całe.

44 Rozporządzenie eIDAS 2.0 (2024/1183) w motywie 7 stwierdza, że zharmonizowane podejście ma na celu „zmniejszenie ryzyka i kosztów wynikających z obecnej fragmentacji spowodowanej stosowaniem rozbieżnych rozwiązań krajowych". Rozporządzenie wykonawcze 2024/2981 dotyczące certyfikacji podkreśla, że wymogi muszą być zharmonizowane we wszystkich państwach członkowskich, „aby zapobiec fragmentacji rynku i stworzyć solidne ramy". Akty wykonawcze (np. 2024/2979, 2024/2982) ustanawiają jednolite specyfikacje techniczne, protokoły i wymogi bezpieczeństwa (np. dotyczące odporności na ataki o wysokim potencjale), które są niezbędne dla funkcjonowania ekosystemu. Regulacje kładą nacisk na to, aby procedury weryfikacji tożsamości (np. przy wydawaniu certyfikatów kwalifikowanych) były przeprowadzane w „równoważny sposób" przez wszystkich dostawców, co zapewnia wiarygodność wyników. Choć termin „model federacyjny" pojawia się częściej w dokumentach technicznych (jak *Architecture and Reference Framework*), regulacje prawne bezpośrednio adresują ryzyka związane z koncentracją danych i potrzebą ochrony relacji między uczestnikami. Przepisy wprowadzają zabezpieczenia (art. 5a ust. 14 rozporządzenia 910/2014), które zabraniają dostawcom portfeli łączenia danych identyfikujących osobę z innymi danymi z usług trzecich (chyba że za zgodą użytkownika), co mityguje ryzyko nadmiernej koncentracji wiedzy o użytkowniku po stronie dostawcy tożsamości. Dokument *Architecture and Reference Framework* (Outline) ilustruje złożoność ekosystemu, w którym uczestniczą różni aktorzy: wydawcy portfeli, dostawcy PID, dostawcy atrybutów (QEAA/EAA) oraz strony ufające. Skuteczna interakcja między tymi niezależnymi podmiotami wymaga „wspólnych protokołów i interfejsów" zdefiniowanych w prawie, aby zapewnić wzajemne zaufanie.

45 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe.

W konsekwencji federację tożsamości należy postrzegać jako model pośredni pomiędzy scentralizowanym zarządzaniem tożsamością a normatywnymi ramami tożsamości cyfrowej, jakie wprowadza prawo Unii Europejskiej. Jej znaczenie polega na wykazaniu, że tożsamość cyfrowa może funkcjonować w sposób ponadorganizacyjny i relacyjny, jednak pełna realizacja tego potencjału wymaga wsparcia w postaci jednolitych regulacji oraz infrastruktury zaufania, co prowadzi do analizy modelu eIDAS jako kolejnego etapu rozwoju zarządzania tożsamością cyfrową.

2.9. Model normatywny Unii Europejskiej – eIDAS i eIDAS2

Regulacje eIDAS oraz ich rozwinięcie w postaci eIDAS2 wprowadzają jakościowo odmienny model zarządzania tożsamością cyfrową, który nie może być utożsamiany ani z rozwiązaniami organizacyjnymi (IAM, CIAM), ani z modelami czysto relacyjnymi, takimi jak federacja tożsamości. Na gruncie prawa Unii Europejskiej tożsamość cyfrowa zostaje bowiem ujęta jako element infrastruktury zaufania, którego funkcjonowanie jest normatywnie określone i którego celem jest zapewnienie skutków prawnych identyfikacji elektronicznej w relacjach transgranicznych[46].

Istotą modelu eIDAS jest oddzielenie tożsamości cyfrowej od pojedynczego dostawcy usługi lub organizacji oraz zapewnienie jej uznawalności przez różne strony ufające, zarówno publiczne, jak i prywatne. W przeciwieństwie do IAM i CIAM, w których tożsamość pozostaje podporządkowana interesom konkretnego podmiotu, eIDAS wprowadza ramy prawne umożliwiające poleganie na wynikach identyfikacji elektronicznej niezależnie od relacji organizacyjnej pomiędzy użytkownikiem a stroną ufającą. Oznacza to, że zarządzanie tożsamością cyfrową zostaje przeniesione na poziom systemowy i regulacyjny, a nie pozostawione wyłącznie praktyce rynkowej[47].

Rozwinięcie regulacji eIDAS w postaci eIDAS2 wzmacnia normatywny charakter tego modelu poprzez dalsze rozczłonkowanie funkcji tożsamości cyfrowej. W szczególności akcentuje się odrębność pomiędzy identyfikacją osoby, potwierdzaniem poszczególnych atrybutów oraz mechanizmami uwierzytelniania. Takie podejście umożliwia odejście od modelu „całościowej identyfikacji" na rzecz selektywnego ujawniania atrybutów, adekwatnych do konkretnego celu lub transakcji. Jednocześnie wzmacnia ono pozycję użytkownika jako podmiotu, który powinien sprawować realną kontrolę nad wykorzystaniem swojej tożsamości cyfrowej[48].

Z perspektywy zarządzania tożsamością cyfrową kluczowe znaczenie ma fakt, że eIDAS i eIDAS2 nie regulują jedynie warstwy technicznej, lecz ustanawiają minimalne wymagania dotyczące zaufania, bezpieczeństwa oraz odpowiedzialności uczestników systemu. Model ten zakłada istnienie jasno określonych ról – użytkownika, dostawcy środków identyfikacji oraz stron ufających – a także mechanizmów umożliwiających ocenę wiarygodności identyfikacji elektronicznej. W ten sposób eIDAS tworzy normatywną ramę zarządzania tożsamością, w której skuteczność identyfikacji nie wynika z pozycji rynkowej dostawcy, lecz z jej zgodności z określonymi standardami prawnymi[49].

Znaczenie modelu eIDAS jest szczególnie widoczne w sektorze bankowym, gdzie instytucje finansowe występują jednocześnie w roli stron ufających oraz podmiotów objętych szczególnymi obowiązkami regulacyjnymi. W tym kontekście eIDAS umożliwia wykorzystanie tożsamości cyfrowej jako instrumentu realizacji obowiązków prawnych, przy jednoczesnym ograniczeniu konieczności tworzenia i utrzymywania własnych, zamkniętych systemów identyfikacyjnych. Analizy praktyki instytucjonalnej wskazują, że wdrożenie normatywnego modelu tożsamości cyfrowej sprzyja zwiększeniu interoperacyjności oraz redukcji fragmentaryzacji rozwiązań stosowanych przez poszczególne instytucje finansowe[50].

W konsekwencji eIDAS i eIDAS2 należy postrzegać jako kulminację ewolucji modeli zarządzania tożsamością cyfrową, w której rozwiązania organizacyjne i relacyjne zostają uzupełnione, a częściowo zastą-

46 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

47 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

48 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

49 Walidacja tożsamości jest procesem opartym na standardach. Źródła wskazują na konieczność stosowania wspólnych protokołów, interfejsów i formatów danych (np. dla atrybutów czy podpisów), co gwarantuje interoperacyjność i pewność prawną w całej Unii, niezależnie od tego, kto technicznie dostarcza rozwiązanie. Rozporządzenie wykonawcze komisji (UE) 2024/2979 art. 7 ust. 4 i art. 8 oraz załącznik III pkt. 3 i załącznik IV pkt. 1; eIDAS 2.0 art. 1ust. 5 (art. 5a ust. 4 lit. f–g, ust. 5 lit. a).

50 D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., całe.

pione przez jednolite ramy prawne o charakterze ponadnarodowym. Model normatywny Unii Europejskiej redefiniuje zarządzanie tożsamością cyfrową, przesuwając punkt ciężkości z kontroli organizacyjnej i kontraktowej na systemowe zaufanie oparte na prawie, co stanowi fundament dalszego rozwoju tożsamości cyfrowej w bankowości i innych sektorach regulowanych[51].

2.10. Porównanie modeli zarządzania tożsamością cyfrową

Przedstawione wcześniej modele zarządzania tożsamością cyfrową – IAM, CIAM, federacja tożsamości oraz model normatywny Unii Europejskiej oparty na regulacjach eIDAS i eIDAS2 – nie stanowią wariantów tego samego rozwiązania technologicznego, lecz reprezentują odmienne koncepcje organizacji zaufania, kontroli nad atrybutami oraz uznawalności skutków identyfikacji elektronicznej. Ich porównanie pozwala uchwycić zasadniczą ewolucję: od modeli wewnątrzorganizacyjnych, przez relacyjne, aż do systemowych i regulacyjnych ram ponadnarodowych[52].

W modelu IAM kontrola nad tożsamością pozostaje w pełni po stronie organizacji. Tożsamość użytkownika ma charakter techniczny i służy wyłącznie realizacji celów bezpieczeństwa w obrębie konkretnego systemu[53].

Model CIAM rozszerza tę logikę na relacje z klientami zewnętrznymi, lecz nadal zachowuje centralną kontrolę dostawcy usług nad zakresem atrybutów i sposobem ich wykorzystania. Użytkownik posiada funkcjonalną możliwość zarządzania kontem, jednak nie sprawuje realnej kontroli nad architekturą tożsamości[54].

W modelu federacyjnym kontrola zostaje częściowo rozproszona – podmioty uzgadniają wzajemne uznawanie wyników identyfikacji, jednak nadal opiera się to na relacjach kontraktowych i technicznych, a nie na jednolitych podstawach normatywnych[55].

Dopiero model eIDAS/eIDAS2 wprowadza systemowe ramy, w których tożsamość cyfrowa przestaje być elementem infrastruktury konkretnej organizacji, a staje się elementem infrastruktury zaufania opartej na prawie. Kontrola nad tożsamością zostaje zinstytucjonalizowana, a jej skuteczność wynika ze zgodności z określonymi standardami regulacyjnymi[56].

IAM oraz CIAM mają charakter zasadniczo zamknięty. Tożsamość nie jest przenoszalna między podmiotami i nie wywołuje skutków poza daną strukturą organizacyjną. Federacja tożsamości umożliwia interoperacyjność pomiędzy określonymi uczestnikami porozumienia, jednak jej zakres jest ograniczony do sieci relacyjnej i zależny od przyjętych standardów technicznych. Model wskazany poprzez eIDAS wprowadza interoperacyjność transgraniczną jako cel regulacyjny, zapewniając uznawalność środków identyfikacji elektronicznej w całej Unii Europejskiej. Interoperacyjność nie jest tu efektem dobrowolnej współpracy rynkowej, lecz obowiązku normatywnego. W modelach IAM i CIAM identyfikacja elektroniczna ma znaczenie funkcjonalne – umożliwia dostęp do systemu lub usługi. Jej skutki prawne ograniczają się do relacji kontraktowej pomiędzy użytkownikiem a dostawcą. Federacja tożsamości rozszerza zakres uznawalności identyfikacji, lecz nadal pozostaje w sferze uzgodnień między podmiotami. Rozporządzenie eIDAS nadaje identyfikacji elektronicznej charakter normatywny, jej skuteczność wynika z regulacji prawa Unii Europejskiej, a nie wyłącznie z relacji organizacyjnych. Tożsamość cyfrowa staje się elementem systemu prawnego, a nie wyłącz-

51 Dokument ramowy („Outline") wymienia „Digital Finance" jako jeden z kluczowych przypadków użycia (*use cases*), który ma ułatwić uwierzytelnianie płatności i zapewnić ich wysoki stopień bezpieczeństwa w oparciu o portfel tożsamości.

52 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe; P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., całe.

53 Tamże.

54 Tamże.

55 Model eIDAS precyzyjnie definiuje uczestników systemu i ich wzajemne relacje prawne. Użytkownik: Zdefiniowany jako osoba fizyczna lub prawna korzystająca z usług zaufania lub środków identyfikacji. Użytkownik ma mieć pełną kontrolę nad swoimi danymi. Dostawca środków identyfikacji (portfela/PID): Podmiot odpowiedzialny za wydanie portfela lub danych identyfikujących osobę. Musi on spełniać szereg wymogów prawnych, w tym dotyczących logicznego oddzielenia danych i zakazu śledzenia użytkowników. Strona ufająca: Podmiot (publiczny lub prywatny), który polega na portfelu w celu świadczenia usług. Strona ufająca musi się zarejestrować, zadeklarować cel użycia danych i podlega weryfikacji tożsamości wobec użytkownika. Rozporządzenie wykonawcze komisji (UE) 2024/2979 art. 1–2; eIDAS 2.0 art. 1 ust. 2 lit. a–b, ust. 3 lit. c–d, ust. 4 (art. 5, 5a, 5b), Rozporządzenie wykonawcze komisji (UE) 2025/848, całe.

56 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe; P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., całe.

nie narzędziem technologicznym. W IAM użytkownik jest biernym podmiotem przypisanym do struktury organizacyjnej. W CIAM jego rola zostaje wzmocniona w wymiarze operacyjnym (zarządzanie kontem), lecz nie strukturalnym.

Federacja tożsamości zwiększa mobilność użytkownika, lecz nadal nie zapewnia mu pełnej autonomii. W rozporządzeniu eIDAS2, zwłaszcza w kontekście portfeli tożsamości cyfrowej, przesuwa punkt ciężkości w stronę większej kontroli użytkownika nad udostępnianiem atrybutów, co zbliża system do koncepcji *self-sovereign identity*, przy jednoczesnym zachowaniu ram regulacyjnych[57].

Tabela 1. Tabela porównawcza modeli zarządzania tożsamością cyfrową.

Kryterium	IAM	CIAM	Federacja tożsamości	eIDAS/eIDAS2
Stopień centralizacji	Wysoki (organizacyjny)	Wysoki (dostawca usług)	Średni (rozproszony kontraktowo)	Systemowy, regulacyjny
Kontrola nad atrybutami	Organizacja	Dostawca usług	Współdzielona	Regulacyjnie określona, z rosnącą rolą użytkownika
Interoperacyjność	-	Ograniczona	Uzgodniona w ramach federacji	Obowiązkowa, transgraniczna
Przenoszalność tożsamości	-	-	Ograniczona	Tak (w ramach UE)
Znaczenie prawne identyfikacji	Wewnętrzne	Kontraktowe	Relacyjne	Normatywne (prawo UE)
Typ zaufania	Organizacyjne	Platformowe	Sieciowe	Systemowe, prawne
Zastosowanie w bankowości	Zarządzanie dostępem	Obsługa klientów	Integracje usług	Transgraniczna identyfikacja i realizacja obowiązków regulacyjnych

Źródło: opracowanie własne na podstawie danych GUS

Analiza porównawcza prowadzi do trzech zasadniczych wniosków (zob. tab. 1):

1. Modele organizacyjne (IAM, CIAM) koncentrują się na kontroli dostępu, a nie na normatywnym zarządzaniu tożsamością w obrocie prawnym.

2. Federacja tożsamości stanowi etap przejściowy, umożliwiający relacyjną interoperacyjność, lecz bez jednolitego fundamentu regulacyjnego.

3. Model eIDAS redefiniuje zarządzanie tożsamością cyfrową, przenosząc je z poziomu organizacyjnego i kontraktowego na poziom systemowy, oparty na prawie i zaufaniu instytucjonalnym.

Z perspektywy sektora bankowego różnice te nie mają wyłącznie charakteru teoretycznego. W warunkach rosnącej regulacji (PSD2, DORA, NIS2) oraz konieczności zapewnienia transgranicznej uznawalności identyfikacji, modele organizacyjne okazują się niewystarczające. Ewolucja w kierunku normatywnych ram tożsamości cyfrowej stanowi zatem nie tylko zmianę technologiczną, lecz także zmianę paradygmatu zarządzania ryzykiem, odpowiedzialnością i zaufaniem w środowisku cyfrowym[58].

2.11. Wyzwania związane z uwierzytelnianiem klientów banku

2.11.1. Uwierzytelnianie jako krytyczny element relacji bank–klient

W praktyce bankowej to nie sam model zarządzania tożsamością cyfrową, lecz mechanizmy uwierzytelniania klientów decydują o rzeczywistym poziomie bezpieczeństwa, dostępności usług oraz możliwości wywoływania skutków prawnych w obrocie elektronicznym.

Uwierzytelnianie klientów banku stanowi centralny element relacji pomiędzy instytucją finansową a użytkownikiem usług cyfrowych. Niezależnie od przyjętego modelu zarządzania tożsamością – organizacyjnego, federacyjnego czy normatywnego – to właśnie mechanizm uwierzytelniania przesądza o tym, czy dana osoba uzyska dostęp do rachunku, będzie mo-

57 Tamże.

58 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe; P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

gła zainicjować transakcję lub złożyć oświadczenie woli w formie elektronicznej. W tym sensie uwierzytelnianie pełni funkcję bramy do obrotu finansowego, a jego skuteczność i wiarygodność mają bezpośrednie przełożenie na bezpieczeństwo środków oraz zaufanie do systemu bankowego[59].

Z perspektywy prawnej uwierzytelnianie nie jest jedynie czynnością techniczną, lecz mechanizmem umożliwiającym powiązanie określonych działań z konkretnym podmiotem prawa. W literaturze przedmiotu podkreśla się, że to właśnie na etapie uwierzytelnienia następuje praktyczna materializacja tożsamości cyfrowej, rozumianej jako zestaw atrybutów wykorzystywanych w danym kontekście usługowym. Błędne lub niewystarczające uwierzytelnienie prowadzi nie tylko do ryzyk bezpieczeństwa, lecz także do podważenia skutków prawnych czynności dokonywanych drogą elektroniczną[60].

2.11.2. Bezpieczeństwo a użyteczność – napięcie strukturalne

Jednym z podstawowych wyzwań związanych z uwierzytelnianiem klientów banku jest konieczność równoważenia wymogów bezpieczeństwa z użytecznością usług cyfrowych. Z jednej strony banki są zobowiązane do stosowania mechanizmów skutecznie chroniących dostęp do rachunków i transakcji, z drugiej zaś – do zapewnienia klientom wygodnego i dostępnego sposobu korzystania z usług. Nadmierna złożoność procedur uwierzytelniania może prowadzić do rezygnacji użytkowników z kanałów cyfrowych lub do obchodzenia zabezpieczeń, co paradoksalnie obniża poziom bezpieczeństwa[61].

W praktyce bankowej napięcie to ujawnia się szczególnie w środowisku bankowości mobilnej, gdzie oczekiwania użytkowników w zakresie szybkości i prostoty obsługi są wyjątkowo wysokie. Mechanizmy uwierzytelniania muszą zatem spełniać jednocześnie funkcję ochronną i usługową, co czyni ich projektowanie jednym z najbardziej problematycznych obszarów cyfryzacji bankowości[62].

2.11.3. Wieloskładnikowe uwierzytelnianie i jego ograniczenia

W odpowiedzi na rosnące zagrożenia bezpieczeństwa banki powszechnie stosują wieloskładnikowe uwierzytelnianie, łączące różne kategorie czynników, takie jak wiedza, posiadanie lub cechy użytkownika. Rozwiązania te zwiększają odporność systemów na nieautoryzowany dostęp, jednak nie eliminują wszystkich ryzyk związanych z uwierzytelnianiem elektronicznym[63].

W literaturze wskazuje się, że wieloskładnikowe uwierzytelnianie może prowadzić do tzw. zmęczenia uwierzytelnianiem, w którym użytkownicy postrzegają kolejne kroki weryfikacji jako uciążliwe i nieproporcjonalne do wykonywanej czynności. Ponadto część mechanizmów, mimo formalnej wieloskładnikowości, pozostaje podatna na ataki socjotechniczne lub kompromitację jednego z czynników, co ogranicza ich skuteczność w praktyce[64]. Z drugiej strony, przy silnym uwierzytelnieniu wieloskładnikowe uwierzytelnienie jest wymagane przepisami prawa. Stąd pojawia się pytanie, czy biometria, a właściwie mechanizmy oparte o biometrię, nie byłyby optymalnym rozwiązaniem.

Biometria stanowi jeden z najbardziej dynamicznie rozwijających się obszarów uwierzytelniania w bankowości. Jej zastosowanie pozwala na odejście od tradycyjnych haseł i kodów na rzecz mechanizmów opartych na cechach użytkownika, co znacząco poprawia wygodę korzystania z usług. Jednocześnie biometria wiąże się z istotnymi ryzykami, wynikającymi z nieodwracalnego charakteru cech biometrycznych oraz możliwości ich wtórnego wykorzystania w przypadku naruszenia bezpieczeństwa systemu. Analizy praktyki bankowej pokazują, że choć biometria zwiększa komfort użytkowników, jej wdrażanie wymaga szczególnej ostrożności oraz uzupełnienia o dodatkowe mechanizmy kontroli

59 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

60 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

61 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe.

62 Tamże.

63 Tamże.

64 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

i zabezpieczenia, aby uniknąć nadmiernej ingerencji w sferę prywatności klientów[65]. Z drugiej strony, dobrze wykorzystane narzędzia oparte o biometrię lub dane behawioralne zmniejszają ryzyko fraudów.

2.12. Prywatność i proporcjonalność jako ograniczenia projektowe uwierzytelniania

Procesy uwierzytelniania klientów banku stanowią istotny punkt styku pomiędzy wymogami bezpieczeństwa a ochroną prywatności użytkowników. Mechanizmy te opierają się na przetwarzaniu danych, które – w zależności od zastosowanego rozwiązania – mogą mieć charakter wrażliwy lub trudny do zmiany po ewentualnym naruszeniu bezpieczeństwa. W konsekwencji uwierzytelnianie nie może być projektowane wyłącznie z perspektywy skuteczności technicznej, lecz musi uwzględniać proporcjonalność stosowanych środków oraz ich wpływ na sferę informacyjną klienta[66].

W literaturze podkreśla się, że nadmierna intensyfikacja mechanizmów uwierzytelniania może prowadzić do nieuzasadnionego rozszerzenia zakresu przetwarzanych danych, w szczególności w sytuacjach, w których poziom ryzyka nie uzasadnia stosowania najbardziej inwazyjnych rozwiązań. Dotyczy to zwłaszcza metod opartych na cechach użytkownika, takich jak biometria, które ze względu na swoją trwałość i trudność zmiany wymagają szczególnie ostrożnego podejścia projektowego[67].

Z perspektywy praktyki bankowej wyzwanie polega zatem na takim doborze mechanizmów uwierzytelniania, aby zakres ingerencji w prywatność klienta pozostawał adekwatny do charakteru wykonywanej czynności, przy jednoczesnym zachowaniu wymaganego poziomu bezpieczeństwa. Napięcie to nie znajduje jednoznacznego rozwiązania technicznego i stanowi trwałą cechę projektowania systemów uwierzytelniania w bankowości cyfrowej, co dodatkowo komplikuje proces ich standaryzacji i skalowania w środowisku usług masowych[68].

Zidentyfikowane ograniczenia projektowe pokazują, że wyzwania związane z uwierzytelnianiem klientów banku nie wynikają wyłącznie z technologii, lecz są konsekwencją szerszych uwarunkowań regulacyjnych i rynkowych, które determinują kierunki dalszego rozwoju tego obszaru[69].

2.13. Trendy regulacyjne i technologiczne

2.13.1. Zmiana paradygmatu regulacyjnego w podejściu do tożsamości i uwierzytelniania

W ostatnich latach obserwuje się wyraźną zmianę paradygmatu regulacyjnego w podejściu do tożsamości cyfrowej i uwierzytelniania użytkowników, polegającą na odejściu od rozwiązań projektowanych wyłącznie na potrzeby pojedynczych organizacji na rzecz systemowych ram zaufania o charakterze ponadsektorowym i transgranicznym. Na gruncie prawa Unii Europejskiej tożsamość cyfrowa przestaje być traktowana jako wewnętrzny zasób podmiotu świadczącego usługę, a zaczyna pełnić funkcję elementu infrastruktury umożliwiającej bezpieczne i prawnie skuteczne uczestnictwo w obrocie elektronicznym[70].

Zmiana ta znajduje bezpośrednie odzwierciedlenie w ewolucji regulacji eIDAS, które przesuwają punkt ciężkości z technicznego potwierdzania tożsamości na normatywne ukształtowanie relacji zaufania pomiędzy użytkownikiem, dostawcą środków identyfikacji oraz stroną ufającą. W tym ujęciu uwierzytelnianie nie jest już wyłącznie mechanizmem kontroli dostępu, lecz staje się elementem warunkującym możliwość wywoływania skutków prawnych czynności dokonywanych drogą elektroniczną. Oznacza to, że znaczenie uwierzytelniania oceniane jest nie tylko przez pryzmat skuteczności technicznej, lecz także przez zdolność do spełnienia określonych standardów zaufania i odpowiedzialności[71].

65 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe.

66 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

67 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe.

68 Tamże.

69 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 6–9 oraz 22–25; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

70 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

71 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

W porównaniu z wcześniejszymi rozwiązaniami sektorowymi, w szczególności stosowanymi w bankowości modelami IAM i CIAM, podejście regulacyjne Unii Europejskiej zmierza do rozczłonkowania funkcji tożsamości cyfrowej oraz do ograniczenia zależności użytkownika od jednego dostawcy usług. Regulacje te sprzyjają rozdzieleniu identyfikacji, potwierdzania atrybutów oraz uwierzytelniania, co ma na celu zwiększenie interoperacyjności systemów oraz wzmocnienie pozycji użytkownika jako podmiotu kontroli nad własnymi danymi. Taki kierunek zmian stanowi reakcję na ograniczenia modeli organizacyjnych, które nie zapewniały ani przenoszalności tożsamości, ani jej uznawalności w szerszym kontekście usługowym[72].

Z perspektywy sektora bankowego zmiana paradygmatu regulacyjnego oznacza stopniowe przesunięcie roli instytucji finansowych z podmiotów samodzielnie zarządzających tożsamością klientów w kierunku stron ufających funkcjonujących w szerszym ekosystemie zaufania. Banki jako podmioty o wysokim poziomie regulacyjnym i zaufania społecznego, pozostają kluczowymi uczestnikami tych procesów, jednak coraz częściej działają w ramach ram wyznaczanych przez rozwiązania o charakterze systemowym, a nie wyłącznie sektorowym. W konsekwencji regulacyjne podejście do tożsamości i uwierzytelniania staje się jednym z głównych czynników determinujących kierunki rozwoju technologicznego w bankowości cyfrowej[73].

2.14. W kierunku uwierzytelniania atrybutowego i kontekstowego

Jednym z kluczowych trendów regulacyjno-technologicznych w obszarze tożsamości cyfrowej jest odejście od modelu pełnej identyfikacji użytkownika na rzecz uwierzytelniania opartego na potwierdzaniu wybranych atrybutów, adekwatnych do konkretnego celu lub transakcji. W tym ujęciu centralnym pytaniem przestaje być „kim jest użytkownik? ", a staje się nim „czy użytkownik spełnia określone warunki? ", takie jak posiadanie odpowiednich uprawnień, osiągnięcie wymaganego wieku czy status klienta. Takie podejście pozwala ograniczyć zakres przetwarzanych danych oraz zmniejszyć ekspozycję użytkownika na ryzyka związane z nadmiernym ujawnianiem informacji identyfikacyjnych[74].

Trend ten znajduje uzasadnienie zarówno w analizach doktrynalnych, jak i w kierunkach rozwoju ram regulacyjnych Unii Europejskiej, które akcentują zasadę minimalizacji i celowości w projektowaniu procesów identyfikacji i uwierzytelniania. Rozdzielenie identyfikacji osoby od potwierdzania poszczególnych atrybutów umożliwia elastyczne dostosowanie mechanizmów uwierzytelniania do poziomu ryzyka związanego z daną czynnością, bez konieczności każdorazowego ujawniania pełnej tożsamości użytkownika. W tym sensie uwierzytelnianie atrybutowe stanowi odpowiedź na ograniczenia modeli, w których tożsamość była wykorzystywana w sposób całościowy i nieproporcjonalny do celu przetwarzania[75].

Istotnym elementem uwierzytelniania kontekstowego jest również uwzględnienie okoliczności towarzyszących danej interakcji, takich jak rodzaj usługi, kanał dostępu, wartość transakcji czy zachowanie użytkownika w trakcie sesji. W praktyce oznacza to możliwość różnicowania poziomu uwierzytelnienia w zależności od stopnia ryzyka, co pozwala na pogodzenie wymogów bezpieczeństwa z oczekiwaniami użytkowników w zakresie szybkości i wygody obsługi. Z perspektywy bankowości cyfrowej podejście to sprzyja projektowaniu bardziej adaptacyjnych mechanizmów uwierzytelniania, które nie opierają się na jednorazowej, statycznej weryfikacji tożsamości[76].

Jednocześnie w literaturze wskazuje się, że przejście w kierunku uwierzytelniania atrybutowego i kontekstowego rodzi nowe wyzwania związane z zaufaniem do źródeł atrybutów, interoperacyjnością systemów oraz odpowiedzialnością za błędne potwierdzenie określonej cechy użytkownika. Skuteczność tego modelu zależy bowiem nie tylko od technologii, lecz także od istnienia wspólnych ram organizacyjnych i prawnych, które umożliwiają stronom ufającym poleganie na potwierdzonych atrybutach. W tym sensie uwierzytelnianie atrybutowe stanowi istotny krok w kierunku bardziej elastycznego i proporcjonalnego zarządzania tożsamością cyfrową, jednak jego pełna implementacja wymaga dalszego rozwoju ekosystemów zaufania[77].

72 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

73 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., całe.

74 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

75 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

76 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe

77 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., całe.

2.15. Portfele tożsamości cyfrowej jako nowa warstwa uwierzytelniania

Jednym z najbardziej wyrazistych trendów regulacyjno-technologicznych w obszarze tożsamości cyfrowej jest rozwój portfeli tożsamości cyfrowej jako narzędzi pośredniczących pomiędzy użytkownikiem a stronami ufającymi. Portfele te nie stanowią kolejnego systemu identyfikacji w tradycyjnym znaczeniu, lecz pełnią funkcję warstwy zarządzania atrybutami i procesami uwierzytelniania, umożliwiającej użytkownikowi kontrolowane udostępnianie określonych informacji w zależności od kontekstu i celu transakcji[78].

W ujęciu regulacyjnym portfele tożsamości wpisują się w tendencję do rozczłonkowania funkcji tożsamości cyfrowej, polegającą na oddzieleniu identyfikacji osoby od potwierdzania poszczególnych atrybutów oraz mechanizmów uwierzytelniania. Takie podejście sprzyja realizacji zasady minimalizacji danych oraz umożliwia odejście od modelu, w którym dostęp do usług wymaga każdorazowego ujawniania pełnej tożsamości użytkownika. Portfel staje się w tym sensie narzędziem operacjonalizacji uwierzytelniania atrybutowego i kontekstowego, omawianego w poprzednim podrozdziale[79].

Z perspektywy bankowości cyfrowej istotną konsekwencją upowszechnienia portfeli tożsamości jest zmiana roli banku w procesach uwierzytelniania. Bank przestaje być jedynym podmiotem tworzącym i utrzymującym tożsamość klienta, a coraz częściej występuje w roli strony ufającej, polegającej na potwierdzonych atrybutach dostarczanych przez zewnętrzne, regulacyjnie umocowane rozwiązania. Taka zmiana sprzyja interoperacyjności oraz ogranicza konieczność utrzymywania rozbudowanych, zamkniętych systemów identyfikacyjnych, jednak jednocześnie wymaga dostosowania procesów wewnętrznych oraz modeli odpowiedzialności[80].

Jednocześnie w literaturze i analizach instytucjonalnych zwraca się uwagę, że portfele tożsamości nie eliminują wszystkich wyzwań związanych z uwierzytelnianiem. Ich skuteczność zależy bowiem od zaufania do źródeł atrybutów, bezpieczeństwa samego portfela oraz jasnego określenia relacji pomiędzy użytkownikiem, dostawcą portfela a stroną ufającą. W tym kontekście portfele tożsamości należy postrzegać nie jako uniwersalne rozwiązanie problemów uwierzytelniania, lecz jako nową warstwę architektury zaufania, której znaczenie i skuteczność będą zależne od spójności regulacyjnej oraz stopnia interoperacyjności ekosystemu, w którym funkcjonują[81].

2.16. Biometria nowej generacji i uwierzytelnianie ciągłe

Współczesne kierunki rozwoju uwierzytelniania w bankowości cyfrowej wskazują na stopniowe odchodzenie od modeli opartych na jednorazowej weryfikacji użytkownika w chwili logowania na rzecz podejść, w których bezpieczeństwo jest utrzymywane w sposób ciągły w trakcie całej sesji. W tym kontekście biometria – rozumiana jako rozpoznawanie użytkownika na podstawie cech fizycznych lub behawioralnych – staje się jednym z kluczowych komponentów architektur bezpieczeństwa w kanałach zdalnych, w szczególności mobilnych, gdzie presja na ergonomię użycia i skrócenie ścieżek autoryzacyjnych jest wyjątkowo silna[82].

Z perspektywy inżynierii systemów biometrycznych podstawowe znaczenie zachowuje rozróżnienie pomiędzy weryfikacją (1:1) a identyfikacją (1:N). W praktyce bankowej dominujące zastosowanie ma model weryfikacji, w którym użytkownik „zgłasza" tożsamość (np. poprzez konto w aplikacji), a system jedynie potwierdza, czy dostarczona próbka odpowiada wzorcowi przypisanemu do tej osoby. Ten wariant jest preferowany ze względu na przewidywalność czasową i operacyjną oraz możliwość ograniczania ryzyka błędnego dopasowania w środowisku usług masowych. Jednocześnie literatura podkreśla, że dla oceny skuteczności biometrii kluczowe znaczenie mają parametry jakości i odporności algorytmów

78 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

79 P. Ruiu, S. Saiu, E. Grosso, dz. cyt., całe.

80 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., całe.

81 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

82 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., całe; A. Drosou, D. Tzovaras, Activity and Event Related Biometrics [w] E. Mordini, D. Tzovaras (ed.) Second Genration Biometrics: The Ethical, Legal and Social Context, Springer, 2012, s. 132–134.

oraz standaryzacja testów wydajnościowych i bezpieczeństwa[83].

Równolegle wyraźnie rysuje się trend rozwoju biometrii behawioralnej i rozwiązań określanych jako uwierzytelnianie ciągłe (*continuous authentication*), które analizują sposób działania użytkownika w trakcie sesji, a nie wyłącznie w punkcie wejścia do systemu. W literaturze wskazuje się na kierunki oparte na aktywności użytkownika oraz „miękkich" cechach biometrycznych, które mogą wspierać weryfikację w sposób mniej inwazyjny i mniej angażujący użytkownika, przy jednoczesnym zwiększaniu wykrywalności przejęcia sesji lub użycia konta przez osobę nieuprawnioną[84]. Z perspektywy bankowości cyfrowej stanowi to rozwinięcie klasycznego modelu „jednorazowego uwierzytelnienia", ponieważ ryzyko może materializować się w trakcie trwania sesji, a nie tylko na jej początku[85].

Jednocześnie wdrożenia biometrii nowej generacji nie eliminują wyzwań charakterystycznych dla przetwarzania danych biometrycznych. Z jednej strony podkreśla się konieczność wzmacniania bezpieczeństwa danych biometrycznych i ograniczania ryzyk związanych z utratą kontroli nad wzorcami, z drugiej – potrzebę projektowania rozwiązań w sposób zgodny z zasadami minimalizacji i ochrony prywatności użytkownika. W ujęciu standardów technicznych i dobrych praktyk szczególną rolę odgrywają rozwiązania ograniczające centralne przechowywanie surowych danych biometrycznych oraz wzmacniające integralność danych w procesach zdalnych (np. poprzez mechanizmy kryptograficznego wiązania kontekstu i danych biometrycznych w toku ich przetwarzania)[86]. W konsekwencji biometria nowej generacji powinna być ujmowana jako element szerszej architektury zaufania, a nie jako samodzielny „zamiennik" tradycyjnych poświadczeń[87].

Z punktu widzenia trendów w bankowości elektronicznej biometria pozostaje jednocześnie obszarem o wysokiej dynamice rozwoju i wysokiej wrażliwości: z jednej strony doświadczenia rynkowe wskazują na rosnącą akceptację rozwiązań biometrycznych w kanałach zdalnych oraz ich znaczenie dla komfortu użytkownika, z drugiej – pojawiają się pytania o skalowalność, standaryzację i bezpieczeństwo rozwiązań behawioralnych, które na rynku bankowym nie są jeszcze równie rozpowszechnione jak biometria oparta o odcisk palca lub wizerunek twarzy[88].

2.17. Interoperacyjność i ekosystemy zaufania w bankowości cyfrowej

Jednym z kluczowych kierunków rozwoju tożsamości cyfrowej i uwierzytelniania w bankowości elektronicznej jest stopniowe przechodzenie od rozwiązań projektowanych w ramach pojedynczych organizacji do ekosystemów zaufania, w których wiele podmiotów współdzieli określone role, odpowiedzialności oraz mechanizmy weryfikacji. W takim ujęciu interoperacyjność przestaje być wyłącznie zagadnieniem technicznym, a staje się elementem o znaczeniu systemowym, warunkującym możliwość bezpiecznego i skalowalnego świadczenia usług cyfrowych w środowisku wielopodmiotowym[89].

Z perspektywy regulacyjnej Unii Europejskiej rozwój interoperacyjnych ekosystemów zaufania znajduje swoje umocowanie w podejściu zakładającym rozdzielenie funkcji identyfikacji, uwierzytelniania oraz potwierdzania atrybutów pomiędzy różne podmioty. Banki coraz częściej występują w tym modelu jako strony ufające, polegające na poświadczeniach lub atrybutach dostarczanych przez zewnętrznych, regulacyjnie umocowanych dostawców. Taka architektura sprzyja przenoszalności tożsamości oraz umożliwia ograniczenie duplikacji procesów identyfikacyjnych, jednocześnie wzmacniając znaczenie wspólnych ram zaufania[90].

83 ISO/IEC 2382-37:2022 – Information technology — Vocabulary. Part 37: Biometrics; A. Drosou, D. Tzovaras, dz. cyt., s. 126–134.

84 A. Drosou, D. Tzovaras, dz. cyt., s. 126–134.

85 A. Drosou, D. Tzovaras, dz. cyt., s. 133–134; M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 18–21.

86 ISO/IEC 2382-37:2022 – Information technology — Vocabulary. Part 37: Biometrics; D. Ioannidis, D. Tzovaras, G. D. Mura, M. Ferro, G. Valenza, A. Tognetti, G. Pioggia, Gait and Anthropometric Profi le Biometrics: A Step Forward [w] E. Mordini, D. Tzovaras (ed.) Second Genration Biometrics: The Ethical, Legal and Social Context, Springer, 2012, s. 120–125.

87 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 22–25; D. Ioannidis, D. Tzovaras, G. D. Mura, M. Ferro, G. Valenza, A. Tognetti, G. Pioggia, dz. cyt., s. 120–125; A. Drosou, D. Tzovaras, dz. cyt., s. 133–134.

88 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 6–9 oraz 26–29.

89 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 10–13; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

90 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., s. 10–12.

W kontekście bankowości cyfrowej interoperacyjność ma szczególne znaczenie w środowisku, w którym użytkownik korzysta równolegle z wielu usług finansowych, często oferowanych przez różne instytucje, a granice pomiędzy sektorami ulegają zatarciu. Otwarte modele świadczenia usług, rozwój ekosystemów API oraz integracja usług finansowych z platformami zewnętrznymi powodują, że tożsamość i uwierzytelnianie muszą być projektowane w sposób umożliwiający bezpieczne poleganie na decyzjach uwierzytelniających podejmowanych poza bezpośrednią kontrolą banku. W tym sensie interoperacyjność staje się warunkiem koniecznym dalszej cyfryzacji sektora finansowego[91].

Jednocześnie literatura oraz analizy instytucjonalne wskazują, że rozwój ekosystemów zaufania rodzi nowe wyzwania związane z zarządzaniem odpowiedzialnością, zaufaniem oraz ryzykiem systemowym. W środowisku wielopodmiotowym konieczne staje się jasne określenie ról poszczególnych uczestników, zasad certyfikacji i nadzoru, a także mechanizmów reagowania na incydenty bezpieczeństwa, które mogą mieć skutki wykraczające poza pojedynczą organizację. W szczególności w sektorze bankowym, gdzie skutki błędów uwierzytelniania mogą prowadzić do istotnych strat finansowych i naruszenia zaufania klientów, kwestia ta nabiera wymiaru strategicznego[92].

W tym kontekście biometria nowej generacji, portfele tożsamości cyfrowej oraz mechanizmy uwierzytelniania atrybutowego należy postrzegać jako komponenty większej architektury zaufania, a nie jako autonomiczne rozwiązania. Ich skuteczność zależy bowiem od zdolności do współdziałania z innymi elementami ekosystemu, w tym od istnienia wspólnych standardów, ram prawnych oraz uznawanych modeli odpowiedzialności. Rozwój interoperacyjnych ekosystemów zaufania stanowi zatem jeden z najważniejszych kierunków dalszej ewolucji uwierzytelniania w bankowości cyfrowej, łącząc aspekty technologiczne, regulacyjne i organizacyjne[93].

2.18. Konsekwencje trendów regulacyjnych i technologicznych dla architektury bezpieczeństwa banków

Zidentyfikowane w niniejszym rozdziale trendy regulacyjne i technologiczne wskazują na zasadniczą zmianę sposobu projektowania architektury bezpieczeństwa w bankowości cyfrowej[94]. Uwierzytelnianie klientów przestaje być pojedynczym etapem procesu dostępu do usług, a staje się rozproszoną funkcją systemową, realizowaną na różnych poziomach interakcji użytkownika z systemem[95]. W konsekwencji architektura bezpieczeństwa banków musi uwzględniać jednocześnie mechanizmy identyfikacji, uwierzytelniania, potwierdzania atrybutów oraz ciągłego monitorowania ryzyka w trakcie trwania relacji z klientem[96].

Rozwój portfeli tożsamości cyfrowej, uwierzytelniania atrybutowego oraz biometrii nowej generacji prowadzi do odejścia od monolitycznych modeli bezpieczeństwa na rzecz architektur warstwowych, w których poszczególne komponenty pełnią komplementarne role. W takim ujęciu tradycyjne poświadczenia (np. hasła czy kody jednorazowe) nie znikają całkowicie, lecz tracą status jedynego punktu decyzyjnego. Coraz większe znaczenie zyskują mechanizmy kontekstowe i behawioralne, które pozwalają na dynamiczną ocenę ryzyka oraz adaptacyjne dostosowanie poziomu ochrony do charakteru danej czynności[97].

Z perspektywy organizacyjnej i regulacyjnej oznacza to konieczność integracji funkcji bezpieczeństwa, zarządzania ryzykiem oraz ochrony danych osobowych już na etapie projektowania systemów i procesów. Banki nie mogą traktować uwierzytelniania wyłącznie jako zagadnienia technicznego, lecz muszą uwzględniać jego wpływ na zgodność regulacyjną, doświadczenie użytkownika oraz relacje z podmiota-

91 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 10–13 oraz 30–32; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

92 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., s. 13–16.

93 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 20–25 oraz 30–32; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., s. 10–12 oraz 13–16.

94 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 4–6; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., 7–10.

95 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 18–21; A. Drosou, D. Tzovaras, dz. cyt., s. 132–134.

96 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 22–25; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

97 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 20-25 oraz 30-32; S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., s. 10–12 oraz 13–16.

mi zewnętrznymi funkcjonującymi w ramach ekosystemów zaufania. W szczególności interoperacyjność oraz możliwość polegania na zewnętrznych źródłach atrybutów wymagają jasno zdefiniowanych modeli odpowiedzialności i nadzoru[98].

Jednocześnie wskazane trendy ujawniają napięcie pomiędzy dążeniem do maksymalizacji bezpieczeństwa a koniecznością zachowania proporcjonalności i akceptowalności stosowanych środków[99]. Architektury oparte na ciągłym monitorowaniu zachowań użytkownika oraz analizie danych biometrycznych muszą być projektowane w sposób zapewniający przejrzystość, minimalizację danych oraz ochronę prywatności klientów. W przeciwnym razie mogą one prowadzić do erozji zaufania, które stanowi fundament relacji bank–klient w środowisku cyfrowym[100].

W konsekwencji można stwierdzić, że przyszłość uwierzytelniania w bankowości cyfrowej nie polega na zastąpieniu jednych technologii innymi, lecz na budowie spójnych, wielowarstwowych architektur zaufania, zdolnych do adaptacji w obliczu zmieniających się zagrożeń, oczekiwań użytkowników oraz wymogów regulacyjnych. Trendy omówione w niniejszym rozdziale wyznaczają kierunek tej ewolucji i stanowią punkt odniesienia dla dalszych analiz dotyczących bezpieczeństwa i tożsamości cyfrowej w sektorze finansowym[101].

2.19. Podsumowanie

Przeprowadzona w niniejszym rozdziale analiza trendów regulacyjnych i technologicznych wskazuje na wyraźną ewolucję podejścia do uwierzytelniania w bankowości cyfrowej, polegającą na odejściu od rozwiązań punktowych i silosowych na rzecz interoperacyjnych, wielopodmiotowych ekosystemów zaufania. W tym ujęciu tożsamość cyfrowa, biometria nowej generacji, portfele tożsamości oraz mechanizmy uwierzytelniania atrybutowego nie funkcjonują jako autonomiczne technologie, lecz jako współzależne elementy architektury systemowej, której celem jest zapewnienie bezpieczeństwa, skalowalności oraz zgodności regulacyjnej usług finansowych w środowisku zdalnym.

Jednocześnie wykazano, że rosnące znaczenie interoperacyjności oraz polegania na zewnętrznych źródłach identyfikacji i atrybutów prowadzi do istotnych wyzwań organizacyjnych i regulacyjnych, w szczególności w zakresie zarządzania odpowiedzialnością, nadzoru oraz ochrony danych osobowych. Banki, występując coraz częściej w roli stron ufających w złożonych ekosystemach cyfrowych, muszą integrować zagadnienia bezpieczeństwa, zarządzania ryzykiem i ochrony prywatności już na etapie projektowania architektur i procesów. W tym kontekście przyszłość uwierzytelniania w bankowości cyfrowej należy postrzegać nie jako sekwencję kolejnych „zamian technologii", lecz jako proces budowy adaptacyjnych, warstwowych architektur zaufania, zdolnych do reagowania na zmieniające się zagrożenia, oczekiwania użytkowników oraz ramy regulacyjne.

98 S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe; D. Szostek, R. Prabucki, M. Jakubik, dz. cyt., s. 13–16.

99 Tamże.

100 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 6–9 oraz 22–25; A. Drosou, D. Tzovaras, dz. cyt., s. 132–134.

101 M. Olczak, M. Brakoniecki, M. Wolski, M. Krzyżański, D. Rzęsa, dz. cyt., 20–25 oraz 30–32; A. Drosou, D. Tzovaras, dz. cyt., s. 132–134, S. Lips, N. Vinogradova, R. Krimmer, D. Draheim, dz. cyt., całe.

Rozdział 3. Biometria jako narzędzie identyfikacji i uwierzytelniania

Współczesne paradygmaty bezpieczeństwa systemów teleinformatycznych przechodzą fundamentalną ewolucję, odchodząc od statycznych mechanizmów kontroli dostępu opartych na wiedzy lub posiadaniu na rzecz dynamicznej weryfikacji tożsamości opartej na cechach posiadanych przez użytkownika. Biometria, definiowana jako zautomatyzowane rozpoznawanie osób na podstawie ich unikalnych cech biologicznych lub behawioralnych, stała się kamieniem węgielnym nowoczesnych architektur bezpieczeństwa, w tym modelu Zero Trust[102]. Niniejszy rozdział stanowi analizę teoretycznych i praktycznych aspektów systemów biometrycznych.

Zgodnie literaturą przedmiotu, **biometryczne rozpoznawanie** to *zautomatyzowany proces, który obejmuje akwizycję danych biometrycznych, ekstrakcję cech oraz ich porównanie z wzorcem referencyjnym*[103]. Biometria oferuje silne powiązanie uprawnień z fizyczną osobą użytkownika, eliminując ryzyko współdzielenia poświadczeń.

W architekturze systemów biometrycznych kluczowe jest rozróżnienie dwóch trybów operacyjnych, które choć korzystają z tych samych algorytmów, różnią się logiką biznesową oraz ich złożonością.

Weryfikacja (model 1:1) to proces potwierdzania zgłoszonej tożsamości, odpowiadający na pytanie „Czy jestem tym, za kogo się podaję? ". Wymaga od użytkownika wstępnego zgłoszenia tożsamości (np. poprzez kartę lub login), po czym system porównuje pobraną próbkę wyłącznie z jednym wzorcem przypisanym do tej osoby. Ze względu na stałą i niską złożoność obliczeniową, weryfikacja jest dominującym modelem w systemach kontroli dostępu logicznego (np. bankowość mobilna, logowanie do stacji roboczych) oraz fizycznego, gdzie kluczowy jest krótki czas reakcji i minimalizacja ryzyka fałszywego dopasowania[104].

Z kolei identyfikacja (model 1:N) służy ustaleniu tożsamości w zbiorze danych, odpowiadając na pytanie „Kim jestem?". W tym scenariuszu użytkownik nie deklaruje tożsamości, a jego wzorzec biometryczny jest porównywany ze wszystkimi wzorcami w bazie danych. Proces ten charakteryzuje się wysoką złożonością obliczeniową, zależną od wielkości bazy, oraz wyższym ryzykiem błędu.

W przeciwieństwie do haseł, systemy biometryczne operują na poziomie prawdopodobieństwa. Decyzja o akceptacji opiera się na porównaniu wyniku podobieństwa z ustalonym progiem, co implikuje możliwość wystąpienia błędów[105].

Współczynnik Fałszywej Akceptacji (*False Acceptance Rate, FAR*) określa prawdopodobieństwo, że system biometryczny błędnie zaakceptuje osobę nieuprawnioną jako uprawnioną. Wskaźnik ten oblicza się jako stosunek liczby fałszywych akceptacji do całkowitej liczby prób dostępu przez oszustów. W systemach o wysokim rygorze bezpieczeństwa FAR musi być minimalizowany, co wymuszają standardy takie jak FIDO[106]. W praktyce FAR wyznacza się empirycznie w procedurze testowej poprzez wielokrotne porównywanie próbek pochodzących od różnych osób i zliczanie przypadków, w których dopasowanie przekroczyło przyjęty próg decyzyjny. Formalnie można go zapisać jako iloraz liczby fałszywych akceptacji i liczby wszystkich fałszywych prób. Warto podkreślić, że FAR jest parametrem zależnym od ustawionej wartości progowej oraz od warunków pozyskania danych, jakości sensora biometrycznego, populacji użytkowników i scenariusza użycia. Obniżanie progu zwiększa wygodę użytkownika, ale zwykle podnosi FAR, natomiast podwyższanie progu ogranicza FAR kosztem wzrostu FRR, dlatego dobór punktu pracy ma charakter decyzji zarządczej, w której równoważy się bezpieczeństwo i użyteczność.

Nie istnieje jedna „prawidłowa" wartość FAR dla wszystkich zastosowań, ponieważ akceptowalny poziom ryzyka zależy od krytyczności procesu, wartości chronionych aktywów i modelu zagrożeń. W zastosowaniach o wysokiej wrażliwości, takich

102 Rose, S., et al. (2020). Zero Trust Architecture. NIST Special Publication 800–207.

103 ISO/IEC 2382-37:2022. Information technology — Vocabulary — Part 37: Biometrics. International Organization for Standardization.

104 NIST Special Publication 800–63B. Digital Identity Guidelines: Authentication and Lifecycle Management. National Institute of Standards and Technology, 2017.

105 Jain, A. K., et al. (2016). 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. Pattern Recognition Letters.

106 FIDO Alliance. Biometrics Requirements v3.0. FIDO Alliance Specifications, 2023.

jak uwierzytelnianie do bankowości elektronicznej lub autoryzacja operacji wysokokwotowych, praktyka projektowa dąży do utrzymywania FAR na poziomie rzędu 10–3 lub niższym, przy czym konkretna wartość jest ustalana w ramach analizy ryzyka oraz testów skuteczności algorytmu w docelowych warunkach. Dla przykładu, jeśli FAR wynosi 0,1%), oznacza to średnio jedną fałszywą akceptację na tysiąc fałszywych prób przy danej wartości progowej; przy FAR równym 0,001% byłaby to jedna fałszywa akceptacja na sto tysięcy fałszywych prób. Z tego względu w systemach, w których konsekwencją błędu może być nieuprawniony dostęp do środków lub danych, parametry progowe dobiera się konserwatywnie, a biometria jest często łączona z dodatkowymi sygnałami ryzyka albo mechanizmami wieloskładnikowymi.

Współczynnik Fałszywego Odrzucenia (*False Rejection Rate, FRR*) określa prawdopodobieństwo, że system biometryczny błędnie odmówi dostępu użytkownikowi uprawnionemu, mimo że przedstawiona próbka pochodzi od właściwej osoby. Wskaźnik ten wyznacza się empirycznie w testach, zliczając przypadki odrzuceń wśród prób prawdziwych, a następnie odnosząc je do całkowitej liczby takich prób. FRR jest w praktyce miarą użyteczności rozwiązania, ponieważ bezpośrednio przekłada się na częstotliwość występowania sytuacji, w których klient musi ponowić próbę uwierzytelnienia lub skorzystać z procedury awaryjnej.

Podobnie jak FAR, FRR nie jest parametrem stałym, lecz zależy od ustawionego progu decyzyjnego, jakości sensora i warunków pozyskania danych, a także od zmienności zachowania i fizjologii użytkownika. W konsekwencji dobór wartości progowej systemu biometrycznego wymaga kompromisu między bezpieczeństwem a wygodą, ponieważ zaostrzenie progu w celu ograniczenia FAR zwykle powoduje wzrost FRR. Dla zobrazowania skutków praktycznych można przyjąć, że FRR na poziomie 1% oznacza średnio jedną fałszywą odmowę na sto prawdziwych prób, natomiast FRR rzędu 0,1% oznacza jedną fałszywą odmowę na tysiąc prób. W systemach bankowości elektronicznej, w których liczba uwierzytelnień w jednostce czasu jest bardzo duża, to nawet niska wartość FRR może przekładać się na istotną liczbę incydentów, dlatego w praktyce stosuje się mechanizmy kompensacyjne, takie jak ponowna próba, alternatywna metoda uwierzytelnienia lub tzw. *step-up authentication*, które uruchamiane jest jednak dopiero przy podwyższonym ryzyku.

Współczynnik Błędu Siodłowego (EER) należy rozumieć jako punkt pracy systemu, w którym wartości FAR i FRR są sobie równe. Służy jako uniwersalna metryka porównawcza algorytmów – im niższa wartość EER, tym wyższa wydajność systemu. Wybór punktu pracy jest decyzją biznesową: zaostrzenie kryteriów bezpieczeństwa (niższy FAR) skutkuje zazwyczaj spadkiem wygody użytkowania (wyższy FRR)[107].

3.1. Klasyfikacja metod biometrycznych (fizyczne vs. behawioralne)

Główny podział metod biometrycznych opiera się na naturze mierzonych danych, co pozwala wyróżnić dwie podstawowe kategorie: biometrię anatomii ciała człowieka (biometrię statyczną) oraz biometrię behawioralną. Biometria anatomii ciała człowieka opiera się na pomiarze niezmiennych cech anatomicznych organizmu. Cechy te są zazwyczaj zdeterminowane genetycznie lub kształtują się we wczesnym etapie rozwoju embrionalnego i pozostają relatywnie stałe przez całe życie człowieka.

Kluczowe modalności biometrii statycznej:

- **Rozpoznawanie odcisków palców.** Najstarsza i najpowszechniejsza metoda, która opiera się na analizie minucji (zakończeń i rozwidleń linii papilarnych), a nie porównywaniu całych obrazów. Nowoczesne sensory ultradźwiękowe mapują trójwymiarową strukturę skóry, co podnosi odporność na fałszerstwa.
- **Rozpoznawanie tęczówki oka.** Uważana za jedną z najdokładniejszych metod ze względu na ogromną liczbę cech charakterystycznych (ponad 240 punktów stopnia swobody), które nie zmieniają się znacząco z wiekiem. Wykorzystuje ideę oświetlenia oka za pomocą bliskiej podczerwieni dla potrzeb do uzyskania wzorca tęczówki. Metoda prof. J. Daugmana przekształca obraz w kod binarny, a porównanie odbywa się poprzez analizę różnic w poszczególnych bitach kodów tęczówek[108].
- **Geometria twarzy.** Analiza topografii twarzy (2D, 3D), w tym odległości między kluczowymi punktami (oczy, nos, usta).

107 Jain, A. K., et al. (2016). 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. Pattern Recognition Letters.

108 Daugman, J. (2004). How Iris Recognition Works. IEEE Transactions on Circuits and Systems for Video Technology.

- **Geometria dłoni.** Identyfikacja osobnicza bazuje na analizie kształtu dłoni.
- **Geometria układu naczyń krwionośnych.** Bazuje na wyniku absorpcji światła podczerwonego przez hemoglobinę, co tworzy mapę naczyń krwionośnych.

Warto zaznaczyć, iż ww. modalności cechują się wysoką **trwałością i powszechnością**[109]. Są idealne do jednorazowej weryfikacji tożsamości (np. kontrola graniczna, odblokowanie urządzenia), jednak wymagają aktywnego zaangażowania użytkownika.

Biometria behawioralna koncentruje się na unikalnych wzorcach zachowań i czynności wykonywanych przez jednostkę. W przeciwieństwie do cech fizycznych, dane te mają charakter dynamiczny i są procesami rozciągniętymi w czasie.

Kluczowe modalności biometrii dynamicznej:

- **Dynamika pisania na klawiaturze.** Analiza czasów naciśnięć klawiszy oraz przerw między naciśnięciami kolejnych klawiszy.
- **Dynamika chodu.** Rozpoznawanie sposobu poruszania się, analizowane przez systemy wizyjne lub sensory w urządzeniach mobilnych (akcelerometry).
- **Dynamika głosu.** Analiza cech akustycznych, tempa mówienia i intonacji. Łączy cechy fizyczne (budowa krtani) z behawioralnymi (nawyki językowe).
- **Dynamika podpisu odręcznego.** Badanie prędkości, nacisku i kątów nachylenia pióra podczas składania podpisu.

Główną zaletą ww. modalności jest możliwość ich wykorzystania dla potrzeb **uwierzytelniania ciągłego**. System może monitorować tożsamość użytkownika przez cały czas trwania sesji bez przerywania jego pracy. Cechy te są jednak podatne na zmiany wynikające ze stanu emocjonalnego, zmęczenia lub chorób.

3.2. Biometria tradycyjna w usługach finansowych – zalety i ograniczenia

W ostatnich latach sektor finansowy intensywnie wdraża tradycyjne metody biometryczne (fizyczne) jako narzędzia identyfikacji i uwierzytelniania klientów. Banki i fintechy coraz śmielej korzystają \ biometrii i czynią to aby zwiększyć bezpieczeństwo dostępu do usług i jednocześnie podnieść wygodę użytkowników. Pojawiają się także bankomaty biometryczne – specjalne urządzenia samoobsługowe, które umożliwiają wypłatę gotówki bez użycia karty bankowej i kodu PIN, a zamiast tego wykorzystują biometryczne metody uwierzytelniania klienta. Przykładowo, na rynku funkcjonują bankomaty wyposażone w skanery odcisków palców lub rozwiązania oparte na rozpoznawaniu tęczówki oka.

Jednym z rzeczywistych przykładów technologii tego typu jest system EyeCash oferowany przez firmę IrisGuard, który integruje skaner tęczówki oka z bankomatem (rys. 1).

Pierwsze pilotaże takich rozwiązań prowadzono m.in. w USA i Azji.

Nawiązując do USA w pierwszej kolejności: jednym z udokumentowanych przykładów jest projekt realizowany przez Bank United, który wdrożył bankomaty z rozpoznawaniem tęczówki oka w oddziałach w stanie Teksas, a następnie przeprowadził badanie reakcji użytkowników oraz skuteczności rozwiązania w warunkach operacyjnych[110]. Równolegle rozwiązania biometryczne rozwijano w Azji, w szczególności w Indiach, gdzie w m.in. Axis Bank wprowadził w 2018 r. uwierzytelnianie biometryczne oparte na biometrii tęczówka[111]. Wdrożenia te miały na celu zwiększenie dostępności usług finansowych oraz ograniczenie problemów związanych z niską skutecznością innych modalności biometrycznych w trudnych warunkach środowiskowych.

W sektorze fintechów oraz bankowości cyfrowej biometria znalazła szerokie zastosowanie przede wszystkim w procesach zdalnego onboardingu klientów. Cyfrowe instytucje finansowe wykorzystują rozwiązania polegające na porównaniu wizerunku twarzy klienta z danymi zawartymi w dokumencie tożsamości, często z użyciem materiału wideo oraz

109 Jain, A. K., Deb, D., & Engelsma, J. J. (2021). Biometrics: Trust, but Verify. *arXiv: Computer Vision and Pattern Recognition*. https://arxiv.org/abs/2105.06625.

110 https://www.atmmarketplace.com/news/bank-united-announces-results-of-first-us-iris-recognition-atm-consumer-survey/.

111 https://www.gktoday.in/axis-bank-becomes-india-s-first-bank-to-introduce-iris-authentication-for-aadhaar-based-transactions-through-micro-atms/.

mechanizmów detekcji żywotności. Tego rodzaju praktyki zostały formalnie ujęte w wytycznych Europejskiego Urzędu Nadzoru Bankowego (EBA) dotyczących zdalnego pozyskiwania klientów, w których biometria jest wskazywana jako dopuszczalne narzędzie identyfikacyjne pod warunkiem spełnienia określonych wymogów organizacyjnych i technicznych[112]. Biometria odgrywa również istotną rolę w ekosystemie płatności mobilnych, gdzie autoryzacja transakcji odbywa się na poziomie urządzenia końcowego. Zarówno Apple Pay[113], jak i Google Wallet[114] przewidują wykorzystanie biometrii urządzenia, takiej jak rozpoznawanie twarzy lub odcisku palca, jako jednej z metod potwierdzania tożsamości użytkownika przy realizacji płatności zgodnie z wymaganiami silnego uwierzytelniania klienta.

Rysunek 1. **Bankomat biometryczny**

Źródło: https://www.irisguard.com/iris-hardware/eyecash/

Gwałtowne upowszechnienie biometrycznych metod uwierzytelniania w usługach finansowych wynika z licznych korzyści, jakie one oferują w porównaniu z hasłami czy kartami.

Do najważniejszych zalet należą:

- **Podniesienie bezpieczeństwa.** Dane biometryczne są znacznie trudniejsze do odgadnięcia lub wyłudzenia niż np. hasła. Każdy człowiek posiada unikalne cechy biometryczne, co utrudnia przestępcom podszycie się pod cudzą tożsamość. Biometryczne uwierzytelnienie skutecznie utrudnia m.in. kradzież konta czy przejmowanie sesji, ponieważ nawet uzyskanie przez atakującego loginu i hasła nie wystarczy bez dostępu do cechy biometrycznej klienta. Co więcej, nowoczesne systemy potrafią wykrywać anomalie w cechach biometrycznych – np. niezgodność głosu lub twarzy – i natychmiast alarmować bank o podej-

112 European Banking Authority, Guidelines on the use of Remote Customer Onboarding Solutions, EBA/GL/2022/15, 2022.

113 https://support.apple.com/pl-pl/guide/security/secc5227ff3c/web.

114 https://support.google.com/wallet/answer/12059326.

rzanej aktywności[115]. Dzięki temu biometria nie tylko zapobiega nieautoryzowanemu dostępowi, ale również może służyć do monitorowania transakcji pod kątem nieprawidłowości w czasie rzeczywistym.

- **Wygoda.** Uwierzytelnianie biometryczne eliminuje po stronie użytkownika konieczność pamiętania haseł, PIN-ów czy noszenia kluczy sprzętowych. Logowanie z wykorzystaniem biometrii jest szybkie i z reguły bezproblemowe, co podnosi satysfakcję użytkowników. Ponadto cechy biometryczne nie zgubią się ani nie zostaną zapomniane – użytkownik zawsze „nosi przy sobie" swoje dane uwierzytelniające. Biometria zwiększa także dostępność usług, czego przykładem jest ułatwione korzystanie z bankowości osobom starszym lub z niepełnosprawnościami (dla których obsługa złożonych haseł jest barierą). Co istotne, biometryczna identyfikacja umożliwia *włączenie finansowe* osób nieposiadających tradycyjnych dokumentów[116].
- **Spełnienie wymogów regulacyjnych oraz redukcja kosztów obsługi.** Biometria pomaga bankom spełnić standardy bezpieczeństwa przewidziane prawem i najlepszymi praktykami[117]. W dłuższej perspektywie uwierzytelnianie biometryczne przekłada się na oszczędności – zmniejsza liczbę telefonów do centrum obsługi klienta w sprawie resetu haseł, upraszcza procesy zakładania kont (brak osobistej wizyty w oddziale banku) i skraca czas obsługi klientów. Biometria dodatkowo redukuje straty związane z nadużyciami, co zmniejsza koszty operacyjne banku – każdy udaremniony przypadek oszustwa to uniknięte potencjalne koszty zwrotów i dochodzeń. Lepsze zabezpieczenia i wygoda przekładają się również na lojalność klientów, otóż konsumenci chętniej korzystają z usług, które są zarazem bezpieczne i bezproblemowe. Biometria jest jednym z głównych elementów wdrażania „silnych mechanizmów uwierzytelniania", które są wymagane przez przepisy DORA. Podmioty finansowe są zobowiązane do wdrażania polityk i protokołów dotyczących silnych mechanizmów uwierzytelniania, opartych na odpowiednich standardach[118]. Rozporządzenie Delegowane (UE) 2024/1774 precyzuje, że podmioty muszą stosować metody uwierzytelniania oparte na wiodących praktykach, w szczególności w zakresie zdalnego dostępu do sieci, dostępu uprzywilejowanego oraz dostępu do zasobów wspierających funkcje krytyczne. Wdrożenie biometrii (np. odcisk palca, skan twarzy) jest standardową metodą spełnienia wymogu silnego uwierzytelniania (MFA) i kontroli dostępu fizycznego oraz logicznego, o których mowa w przepisach[119]. Ponadto wymagane jest, aby osoby fizyczne i systemy uzyskujące dostęp do informacji były jednoznacznie zidentyfikowane i uwierzytelnione, co w nowoczesnych systemach często realizuje się poprzez cechy biometryczne[120]. Przetwarzanie danych osobowych (w tym biometrycznych) przez podmioty finansowe oraz ich zewnętrznych dostawców usług ICT musi odbywać się zgodnie z wymogami ochrony danych, co obejmuje zapewnienie poufności i integralności tych danych[121].
- **Spójna identyfikacja w wielu kanałach.** Jedną z istotnych zalet biometrii jest możliwość ujednolicenia sposobu potwierdzania tożsamości klienta we wszystkich kanałach dostępu do usług finansowych. Należy przy tym podkreślić, że banki – zgodnie z PSD2 i RTS w sprawie silnego uwierzytelnienia klienta (SCA) – są zobowiązane do stosowania co najmniej dwóch elementów z trzech niezależnych kategorii (wiedza, posiadanie, cecha klienta). Biometria stanowi jeden z tych elementów (kategoria „cecha klienta") i funkcjonuje w połączeniu z innym czynnikiem, np. urządzeniem klienta lub aplikacją autoryzacyjną. Choć w bankowości internetowej i mobilnej często wykorzystywane są te same dane uwierzytelniające, poszczególne kanały różnią się sposobem interakcji oraz kontekstem ryzyka (oddział, bankomat, infolinia, aplikacja mobilna). Zastosowanie biometrii jako jednego z elementów SCA pozwala wprowadzić spójny model potwierdzania tożsamości niezależnie od kanału – np. biometrię twarzy w aplikacji mobilnej, biometrię głosową w centrum obsługi czy czytnik biometryczny w urządzeniu samoobsługowym – przy zachowaniu wymogów regulacyjnych. Z perspektywy bezpieczeństwa strategia omnichannel ogranicza ryzyko wykorzystywania potencjalnie słabszych procedur w jednym z kanałów do obejścia zabezpieczeń w innym.

115 TechMagic Blog, Biometrics in Banking: Implementation Cases and Benefits, 2023.

116 Lumin Digital, How Biometric Authentication Secures the Future of Digital Banking, 19.05.2022.

117 FinLegalTech, Biometria behawioralna z punktu widzenia instytucji finansowych, 10.01.2020.

118 Art. 9 ust. 4 DORA.

119 Art. 21 Rozporządzenia Delegowanego (UE) 2024/1774.

120 Art. 20 Rozporządzenia Delegowanego (UE) 2024/1774.

121 Motyw 19 preambuły oraz art. 1 Rozporządzenia Delegowanego (UE) 2024/1774.

Dodatkowo biometria umożliwia wdrożenie mechanizmów ciągłego uwierzytelniania (*continuous authentication*), które – choć nie zastępują formalnego SCA – mogą stanowić uzupełniający mechanizm oceny ryzyka w trakcie trwania sesji.

Mimo licznych zalet, fizyczne metody biometryczne niosą ze sobą także istotne ograniczenia i ryzyka, z których banki muszą zdawać sobie sprawę:

- **Podatność na fałszerstwa.** Choć cechy biometryczne są unikalne, w praktyce okazuje się, że nie są one w pełni odporne na podrobienie. Cyberprzestępcy opracowali metody odtwarzania cech fizycznych – przykładowo odcisk palca udało się sklonować na podstawie zdjęcia kciuka o wysokiej rozdzielczości. Popularne zabezpieczenie smartfonów i aplikacji bankowych – odblokowanie odciskiem palca – może więc przy braku dodatkowych zabezpieczeń (jak detekcja żywotności) zostać oszukane za pomocą sztucznie wykonanej kopii odcisku palca. Jeszcze bardziej zaskakujące są doniesienia o łatwości oszukania systemów rozpoznawania twarzy – proste modele potrafią dać się zwieść zwykłej fotografii właściciela lub trójwymiarowej masce. Opisywane ataki prezentacyjne stanowią poważne zagrożenie, dlatego branża opracowała standardy oceny odporności systemów biometrycznych na oszustwa, np. ISO/IEC 30107 określający poziomy zabezpieczeń przed próbami podszycia się. Producenci wdrażają mechanizmy detekcji żywotności, aby odróżnić prawdziwego użytkownika od imitacji. Niemniej wyścig z atakującymi trwa – coraz bardziej zaawansowane sztucznie generowanie wizerunku głosu lub twarzy użytkownika potrafią zdezorientować systemy biometryczne, utrudniając odróżnienie prawdziwej osoby od cyfrowej imitacji[122]. Głośne stały się przypadki spreparowanych nagrań audio imitujących głos prezesów zarządu, czy podrobionych obrazów twarzy generowanych przez sieci przeciwstawne, które omijały standardowe mechanizmy weryfikacji[123].

  W konsekwencji rosnącej skuteczności technik fałszowania cech biometrycznych konieczne staje się systematyczne doskonalenie mechanizmów ochronnych, obejmujących zarówno warstwę sprzętową, jak i programową. W praktyce oznacza to stosowanie metod analizy multispektralnej obrazu twarzy, które bazują na różnicach w absorpcji i odbiciu promieniowania w różnych zakresach widma w celu odróżnienia żywej tkanki od artefaktów syntetycznych lub fizycznych replik. Uzupełnieniem tych podejść są zaawansowane algorytmy detekcji manipulacji wizualnych, analizujące nieciągłości strukturalne obrazu, nienaturalne korelacje pikseli, niespójności oświetlenia oraz subtelne zaburzenia dynamiki obrazu, charakterystyczne dla treści generowanych lub modyfikowanych algorytmicznie. Coraz częściej stosuje się także rozwiązania oparte na uwierzytelnianiu wielomodalnym[124], w których decyzja o tożsamości użytkownika nie opiera się na pojedynczej cesze biometrycznej, lecz na korelacji wielu niezależnych sygnałów, takich jak cechy twarzy, dynamika głosu, wzorce behawioralne oraz kontekst urządzenia i sesji, co istotnie podnosi odporność systemu na próby obejścia pojedynczego mechanizmu ochronnego.

- **Błędy i ograniczenia techniczne.** Systemy biometryczne nie dają 100% pewności poprawnej identyfikacji – działają na zasadzie porównań probabilistycznych, przez co zawsze istnieje ryzyko błędnej decyzji. Banki muszą wyważyć te ryzyka dobierając czułość systemu – zbyt liberalny próg zwiększy poziom błędnej akceptacji i grozi wpuszczeniem oszusta, z kolei zbyt restrykcyjny próg będzie błędnie odrzucał uprawnionych użytkowników. Mimo postępów (np. nowoczesne algorytmy rozpoznawania twarzy osiągają bardzo niski średni błąd EER), w praktyce czynników utrudniających identyfikację jest wiele: zmiany wyglądu osoby, warunki środowiskowe, różnorodność populacji. Te ograniczenia powodują, że zawsze pewien odsetek klientów będzie mieć kłopot z użyciem biometrii, np. osoby starsze lub pracujące fizycznie mogą mieć starty naskórek palca uniemożliwiający skuteczny odczyt linii papilarnych, a osoby z wadami wzroku mogą unikać skanowania tęczówki oka. Należy zatem zapew-

122 Lumin Digital, How Biometric Authentication Secures the Future of Digital Banking, 19.05.2022.

123 W przypadku deepfake głosowych skuteczność ataku nie musi polegać na obejściu automatycznej weryfikacji mówcy, lecz często wynika z oddziaływania na człowieka poprzez wykorzystanie metod i technik inżynierii społecznej (zaufania, autorytetu lub presji). Ataki te są szczególnie groźne w procesach, w których dyspozycje finansowe podejmowane są na podstawie komunikatów przekazywanych kanałem audio. Oznacza to, że nawet systemy o wysokiej skuteczności technicznej nie eliminują ryzyka, jeżeli nie są wsparte odpowiednimi rozwiązaniami natury organizacyjnej. W odniesieniu do deepfake'ów wideo, istotne jest rozróżnienie między atakami prezentacyjnymi a iniekcyjnymi, w których syntetyczny strumień wideo jest podstawiany bezpośrednio do aplikacji. Analizy wskazują, że skuteczność obejścia zabezpieczeń zależy od rodzaju mechanizmu detekcji i warunków jego działania, a brak uniwersalnej metody wykrywania wszystkich form fałszerstw uzasadnia stosowanie architektur wielowarstwowych i łączenie różnych źródeł danych uwierzytelniających.

124 Khan, F. A., Khan, M. K. Generative AI and Deepfake Detection in Biometric Systems. Cogn Comput 17, 112 (2025).

nić alternatywne metody uwierzytelnienia dla tych przypadków, co komplikuje architekturę systemu (wymóg wspierania zarówno biometrii, jak i np. Tradycyjnych metod jako opcji zapasowej).

- **Ryzyka prywatności i ochrona danych.** Dane biometryczne są wrażliwymi danymi osobowymi, podlegającymi restrykcyjnym przepisom o ochronie prywatności. Wdrożenie biometrii wymaga zatem spełnienia wysokich standardów bezpieczeństwa informacji: szyfrowania i zabezpieczenia baz danych, minimalizacji zakresu przetwarzanych danych oraz uzyskania świadomych zgód od klientów na przetwarzanie ich cech biometrycznych. Klienci mogą odczuwać obawy przed nadużyciami – np. czy ich odcisk palca nie zostanie wykorzystany do innego celu lub czy wyciek takich danych nie narazi ich na identyfikację przez osoby trzecie. Szczególnie negatywne skutki może mieć kradzież szablonów biometrycznych z baz – w przeciwieństwie do haseł, cechy biometrycznej nie da się łatwo zmienić. Jeśli np. wycieką wzorce linii papilarnych klientów, mogą one zostać użyte do prób logowania w innych usługach (tzw. przejęcie tożsamości), a użytkownik nie ma możliwości *„resetu”* swojego odcisku palca tak jak zmiany hasła.
- **Koszty wdrożenia i kwestie operacyjne.** Wprowadzenie biometrycznych metod uwierzytelniania wymaga inwestycji w infrastrukturę i integrację z istniejącymi systemami bankowymi. Po stronie klientów niezbędna jest odpowiednia warstwa sprzętowa – czytniki linii papilarnych, kamery wysokiej rozdzielczości, mikrofony wysokiej jakości, ewentualnie skanery tęczówki czy układu żył. Wiele tych sensorów znajduje się już w nowoczesnych smartfonach klientów, co obniża barierę wdrożenia (bank może wykorzystać model BYOD, czyli urządzenia własne użytkownika). Większym wyzwaniem jest integracja biometrii w kanałach fizycznych – np. modernizacja bankomatów lub kas bankowych, aby akceptowały biometrię (instalacja skanerów, szyfrowana transmisja danych). Konieczne jest ponadto przeszkolenie personelu i przygotowanie procedury na wypadek awarii systemu biometrycznego (np. jak obsłużyć klienta, którego cecha nie jest rozpoznawana). Istotne wyzwanie stanowi znalezienie balansu między wygodą a bezpieczeństwem – biometria powinna upraszczać życie użytkownika, ale bank musi być gotów na sytuacje wyjątkowe i ataki, co nieraz komplikuje finalny system (np. dodanie dodatkowych kroków weryfikacji przy podejrzanych okolicznościach).

Podsumowując, tradycyjna biometria (np. odcisk palca, rozpoznawanie twarzy czy głosu) może stanowić istotny element systemów bezpieczeństwa w usługach finansowych, oferując wysoki poziom ochrony przy jednoczesnym zachowaniu wygody użytkownika. W obowiązującym modelu regulacyjnym pełni ona rolę jednego z elementów silnego uwierzytelnienia klienta (SCA), funkcjonując w połączeniu z innymi czynnikami, takimi jak urządzenie klienta czy mechanizmy kryptograficzne. Koncepcja „klient jako hasło” ma zatem charakter metaforyczny – biometria może znacząco ograniczyć zależność od tradycyjnych haseł, lecz nie zastępuje całkowicie wieloskładnikowego modelu bezpieczeństwa wymaganego przez przepisy. Należy również podkreślić, że biometria fizyczna nie stanowi rozwiązania kompletnego. W praktyce musi być wspierana przez dodatkowe mechanizmy, takie jak systemy detekcji nadużyć, analiza kontekstowa ryzyka czy ciągłe uwierzytelnianie behawioralne. To właśnie biometria behawioralna – oparta na analizie wzorców korzystania z urządzenia i dynamiki zachowań – może pełnić funkcję uzupełniającej, „ciągłej” warstwy weryfikacyjnej w trakcie sesji, zwiększając szanse wykrycia przejęcia konta nawet po prawidłowym przejściu formalnego procesu SCA. W efekcie, zarówno biometria tradycyjna, jak i behawioralna powinny być postrzegane jako komplementarne elementy szerszej, wielowarstwowej strategii bezpieczeństwa, a nie jako samodzielne rozwiązania. Kierunek rozwoju nowoczesnej bankowości zmierza raczej w stronę ograniczenia roli statycznych haseł oraz wzmocnienia modelu uwierzytelniania opartego na analizie ryzyka, przy jednoczesnym zachowaniu zgodności z wymogami regulacyjnymi.

3.3. Pojęcie i istota biometrii behawioralnej

Biometria to nauka zajmująca się pomiarem i analizą cech fizycznych oraz behawioralnych ludzi w celu ich identyfikacji lub weryfikacji tożsamości. Podczas gdy biometria anatomii ciała człowieka (tzw. biometria statyczna) koncentruje się na niezmiennych cechach anatomicznych (np. odcisk palca, tęczówka oka), **biometria behawioralna** (dynamiczna) bada unikalne wzorce zachowania człowieka.

Biometria behawioralna definiowana jest jako zbiór technik umożliwiających rozpoznawanie osób na podstawie charakterystycznych cech ich zachowania i sposobu interakcji z otoczeniem lub syste-

mami informatycznymi. Istota tej dziedziny opiera się na założeniu, że procesy motoryczne i nawyki poznawcze jednostki są na tyle unikalne i powtarzalne, iż mogą służyć jako wiarygodny identyfikator[125].

Kluczową różnicą w stosunku do biometrii anatomii ciała jest wymiar czasowy. Cechy anatomii są stałe, natomiast cechy behawioralne są procesami zachodzącymi w czasie. Z tego względu biometria behawioralna często kojarzona jest z koncepcją **uwierzytelniania ciągłego**, zgodnie z którą tożsamość użytkownika jest weryfikowana nie tylko w momencie logowania, ale przez cały czas trwania sesji.

W literaturze przedmiotu wyróżnia się kilka podstawowych kategorii danych behawioralnych, które podlegają analizie:

- **Dynamika pisania na klawiaturze (*Keystroke Dynamics*).** Analiza rytmu uderzeń w klawisze, czasu przytrzymania klawisza (*dwell time*) oraz przerw między naciśnięciami (*flight time*).
- **Dynamika posługiwania się myszką lub ekranem dotykowym.** Badanie trajektorii ruchu kursora, siły nacisku na ekran, prędkości przewijania stron oraz kąta trzymania urządzenia mobilnego.
- **Analiza chodu.** Rozpoznawanie wzorców ruchu ciała podczas chodzenia, analizowane zazwyczaj za pomocą akcelerometrów i żyroskopów wbudowanych w smartfony lub systemów wizyjnych.
- **Biometria głosu.** Co prawda głos posiada cechy fizyczne, to jego modulacja, tempo mówienia i akcent tworzą składową behawioralną.
- **Podpis dynamiczny.** W odróżnieniu od analizy statycznego obrazu podpisu, podpis dynamiczny jest reprezentowany jako wielowymiarowy szereg czasowy rejestrowany przez tablet. Rejestrowane są nie tylko wartości współrzędnych położenia bezprzewodowego pisaka, lecz także charakterystyki dynamiki składanego podpisu: siłę nacisku, parametry orientacji pisaka (kąt elewacji i kąt azymutu) oraz inne sygnały zależne od urządzenia. Wymianę i ujednolicenie struktury takich danych opisuje norma ISO/IEC 19794–7:2021[126], która definiuje formaty interoperacyjnego zapisu danych podpisu dynamicznego jako danych behawioralnych.

Główną zaletą biometrii behawioralnej jest jej nieinwazyjność. Proces weryfikacji może odbywać się w tle, bez konieczności przerywania pracy użytkownika. Dodatkowo, cechy behawioralne są trudniejsze do sfałszowania niż np. odciski palców (które można pobrać z przedmiotów codziennego użytku), ponieważ wymagają odtworzenia dynamicznego procesu fizjologicznego.

Do istotnych wyzwań biometrii behawioralnej należy zmienność osobnicza. Stan zdrowia, zmęczenie, stres czy czynniki zewnętrzne (np. temperatura, niewygodne stanowisko pracy) mogą wpływać na zmianę wzorca zachowania, co zwiększa współczynnik FRR. Zmienność osobnicza w biometrii behawioralnej przekłada się na wahania jakości próbek i stabilności cech w czasie, co wprost wpływa na parametry błędów (w szczególności FRR) oraz na dobór punktu pracy systemu. Z perspektywy standaryzacji oznacza to, że ocena skuteczności powinna być prowadzona według metodyk technicznego testowania i raportowania wyników, w tym z uwzględnieniem błędów oraz warunków testu, zgodnie z zasadami ujętymi w ISO/IEC 19795–1:2021[127]. Jednocześnie, ponieważ zmienność zachowania i warunków środowiskowych wpływa na jakość danych wejściowych, zasadne jest odniesienie do ram oceny i interpretacji jakości próbek biometrycznych w ujęciu ogólnym, opisanych w dokumencie ISO/IEC 29794–1:2024[128].

Istotne są również kwestie etyczne i prywatności, gdyż zbieranie szczegółowych danych o sposobie interakcji z urządzeniem może być postrzegane jako nadmierna inwigilacja.

Wymiar prywatności i ochrony danych wiąże się z tym, że dane behawioralne mogą umożliwiać wnioskowanie o cechach użytkownika lub jego nawykach, dlatego przetwarzanie powinno uwzględniać zasady ochrony danych biometrycznych, w tym wymagania i rekomendacje dotyczące poufności, integralności oraz odwoływalności wzorców, opisane w normie ISO/IEC 24745:2022[129].

125 Jingyuan Zhang and Yan Wang. 2024. A Survey of Behavioral Biometric Authentication on Smartphones. In Proceedings of the 2023 4th International Conference on Machine Learning and Computer Application (ICMLCA '23). Association for Computing Machinery, New York, NY, USA, 722–729. https://doi.org/10.1145/3650215.3650342.

126 https://www.iso.org/standard/77910.html.

127 https://www.iso.org/standard/73515.html.

128 https://www.iso.org/standard/79519.html.

129 https://www.iso.org/standard/75302.html.

Rozdział 4. Biometria behawioralna w praktyce bankowej

4.1. Typowe cechy behawioralne (dynamika klawiatury, ruchy myszą, korzystanie z aplikacji mobilnych, wzorce nawigacji)

Biometria behawioralna wykorzystuje wielowymiarowe dane opisujące sposób interakcji człowieka z urządzeniem lub aplikacją. Badania z obszaru HCI (*Human-Computer Interaction*) pokazują, że sposób wpisywania tekstu, poruszania myszą czy trzymania telefonu tworzy wysoce unikalny wzorzec motoryczno-kognitywny[130].

4.1.1. Dynamika klawiatury (*Keystroke Dynamics*)

Keystroke dynamics jest jedną z najstarszych i najlepiej przebadanych metod biometrii behawioralnej. Polega na analizie czasowych i rytmicznych cech wpisywania tekstu na klawiaturze. Badania prowadzone od lat 80. wskazują, że wzorzec pisania ma charakter indywidualny – relatywnie stabilny dla danej osoby, a jednocześnie trudny do precyzyjnego odtworzenia przez osobę trzecią[131].

Do podstawowych parametrów analizy należą:

- *Dwell Time* – czas trzymania pojedynczego klawisza (od momentu jego naciśnięcia do zwolnienia). Parametr ten odzwierciedla mikroruchy motoryczne użytkownika i jest relatywnie stabilny w dłuższych okresach, choć może ulegać zmianom w sytuacjach skrajnego zmęczenia lub silnych emocji[132].
- *Flight Time* – czas pomiędzy zwolnieniem jednego klawisza a naciśnięciem kolejnego. Parametr ten oddaje płynność i tempo przechodzenia między znakami oraz strukturę rytmiczną pisania. W modelach opartych na sieciach neuronowych (np. RNN, LSTM) wykorzystywany jest jako element sekwencyjny, pozwalający uchwycić temporalny charakter wzorca[133].
- *Analiza n-gramów* – polega na analizie sekwencji kilku kolejnych znaków (np. dwuznaków, trójznaków) wraz z odpowiadającymi im czasami przejść. Pozwala to uchwycić bardziej złożone wzorce rytmiczne i zwiększyć precyzję klasyfikacji, zwłaszcza przy zastosowaniu metod zespołowych (*ensemble methods*)[134].

Warto jednak podkreślić, że dynamika klawiatury nie jest cechą całkowicie niezmienną. Badania eksperymentalne wskazują, że w sytuacjach podwyższonego stresu, presji czasowej lub działania pod przymusem mogą występować mierzalne odchylenia od standardowego wzorca użytkownika. Z jednej strony stanowi to wyzwanie dla stabilności modeli, z drugiej – może być wykorzystane jako dodatkowy sygnał w systemach oceny ryzyka i detekcji nadużyć[135].

130 Teh, P. S.; Teoh, A. B. J.; Yue, S., „A Survey of Keystroke Dynamics Biometrics", The Scientific World Journal, vol. 2013, Article ID 408280, 2013.

131 Gaines, R.; Lisowski, W.; Press, S.; Shapiro, N., Authentication by Keystroke Timing, RAND Corporation, Technical Report R-256-NSF, 1980

132 Janakiraman, R.; Sim, T., „Keystroke Dynamics in a General Setting", w: AVBPA 2007, LNCS 4472, s. 584–593, 2007.

133 Lu, X.; Zhang, S.; Hui, P.; Lió, P., „Continuous Authentication by Free-Text Keystroke Based on CNN and RNN", Computers & Security, vol. 96, 101861, 2020.

134 Killourhy, K. S.; Maxion, R. A., „Comparing Anomaly-Detection Algorithms for Keystroke Dynamics", w: IEEE/IFIP Int. Conf. on Dependable Systems & Networks (DSN), s. 125–134, 2009.

135 Vizer, L. M.; Zhou, L.; Sears, A., „Automated Stress Detection Using Keystroke and Linguistic Features: An Exploratory Study", International Journal of Human-Computer Studies, vol. 67, nr 10, s. 870–886, 2009.

4.1.2. Ruchy myszą i biometria kognitywna

Badania w obszarze analizy ruchów myszy wykazały silne powiązanie pomiędzy trajektorią ruchu a procesami poznawczymi użytkownika[136].

Najważniejsze cechy:

- Ruchy ludzkie charakteryzują się mikrofluktuacjami, podczas gdy boty generują ruchy liniowe lub matematycznie „zbyt idealne"[137].
- Mikrodrżenia korelują z indywidualnymi cechami motorycznymi i są praktycznie niemożliwe do sfałszowania.
- Analiza intencji pozwala wykrywać konflikty kognitywne i manipulacje socjotechniczne poprzez analizę wahań w punktach decyzyjnych[138].

4.1.3. Rozwiązania mobilne

Urządzenia mobilne dostarczają znacznie bogatszy zestaw cech, co potwierdzają liczne badania z zakresu *mobile behavioral biometrics*[139].

Najczęściej analizowane dane:

- Pochodzące z ekranu dotykowego – cechy takie jak siła nacisku, obszar styku czy kierunkowość są unikalne i stabilne[140].
- Pochodzące z sensorów ruchu (np. Akcelerometru lub żyroskopu) – ich analiza umożliwia detekcję: a) przejęcia urządzenia przez napastnika, b) ataków RAT, c) zmian w chwycie telefonu wskazujących na stres lub manipulację[141].
- Dotyczące chodu – szczególnie przydatne dla potrzeb weryfikacji w tle podczas poruszania się użytkownika z urządzeniem[142].

4.2. Mechanizmy gromadzenia i analizy danych

Mechanizmy gromadzenia i analizy danych w systemach biometrii behawioralnej w bankowości cyfrowej są ściśle związane z wymaganiami regulacyjnymi dotyczącymi silnego uwierzytelniania klienta (*Strong Customer Authentication – SCA*) na gruncie dyrektywy PSD2 (*Payment Services Directive 2*) oraz projektowanych aktów PSD3 (*Payment Services Directive 3*) i PSR (*Payment Services Regulation* – rozporządzenie w sprawie usług płatniczych). Jednocześnie podlegają rygorom rozporządzenia RODO/GDPR (*General Data Protection Regulation*) w zakresie przetwarzania danych biometrycznych jako szczególnej kategorii danych osobowych. Mechanizmy te muszą zatem zapewniać wysoką skuteczność wykrywania nadużyć, minimalizować ingerencję w doświadczenie użytkownika (*User Experience – UX*) oraz pozostawać zgodne zarówno z europejskimi wymogami ochrony danych osobowych (RODO), jak i regulacjami dotyczącymi usług płatniczych[143]. W szczególności Dyrektywa (UE) 2015/2366 (PSD2) oraz Rozporządzenie delegowane Komisji (UE) 2018/389 (RTS) nakładają na dostawców usług płatniczych obo-

136 Freeman, J. B.; Ambady, N., „MouseTracker: Software for Studying Real-Time Mental Processing Using a Computer Mouse-Tracking Method", Behavior Research Methods, vol. 42, nr 1, s. 226–241, 2010.

137 Mondal, S.; Bours, P., „Continuous Authentication Using Mouse Dynamics", w: Int. Conf. of the BIOSIG Special Interest Group (BIOSIG), s. 1–12, 2013.

138 Stillman, P. E.; Shen, X.; Ferguson, M. J., „How Mouse-Tracking Can Advance Social Cognitive Theory", Trends in Cognitive Sciences, vol. 22, nr 6, s. 531–543, 2018.

139 Mahfouz, A.; Mahmoud, T. M.; Eldin, A. S., „A Survey on Behavioral Biometric Authentication on Smartphones", Journal of Information Security and Applications, vol. 37, s. 28–37, 2017.

140 Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D., „Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication", IEEE Transactions on Information Forensics and Security, vol. 8, nr 1, s. 136–148, 2013.

141 Acien, A. et al., „Keystroke Mobile Authentication: Performance of Long-Term Approaches and Fusion with Behavioral Profiling", w: IbPRIA 2019, LNCS 11867, s. 91–102, 2019.

142 Mäntyjärvi, J.; Lindholm, M.; Vildjiounaite, E.; Mäkelä, S. M.; Ailisto, H. A., „Identifying Users of Portable Devices from Gait Pattern with Accelerometers", w: ICASSP 2005, 2005.

143 Parlament Europejski i Rada (UE). Rozporządzenie (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO / GDPR). Dziennik Urzędowy UE L 119/1.

wiązek stosowania silnego uwierzytelnienia klienta (SCA), opartego na co najmniej dwóch niezależnych elementach z kategorii wiedzy, posiadania i cech klienta. W tym modelu biometria stanowi jeden z dopuszczalnych elementów (*inherence*), jednak musi funkcjonować w połączeniu z innym czynnikiem oraz spełniać wymogi niezależności i ochrony danych uwierzytelniających[144]. Jednocześnie przetwarzanie danych biometrycznych podlega rygorom RODO, w tym zasadzie minimalizacji danych (art. 5), wymogowi *privacy by design* (art. 25) oraz obowiązkowi zapewnienia odpowiednich środków bezpieczeństwa (art. 32), a w przypadku kwalifikacji jako dane szczególnej kategorii – także ograniczeniom wynikającym z art. 9 RODO.

W literaturze oraz praktyce sektora finansowego przyjmuje się, że pełny cykl przetwarzania danych behawioralnych obejmuje: (1) pozyskiwanie surowych danych, (2) przetwarzanie wstępne i normalizację, (3) ekstrakcję cech, (4) modelowanie i wnioskowanie z wykorzystaniem uczenia maszynowego (*Machine Learning – ML*), (5) fuzję sygnałów i podejmowanie decyzji oraz (6) ciągłą adaptację profilu użytkownika w czasie[145].

4.2.1. Architektura pozyskiwania danych i źródła sygnałów

Większość wdrożeń w bankowości internetowej oraz mobilnej opiera się na architekturze „lekki klient – ciężki serwer", w której kod osadzony w przeglądarce lub aplikacji mobilnej zbiera surowe zdarzenia, a właściwa analiza odbywa się w centralnym silniku analitycznym[146].

Po stronie klienta rejestrowane są m.in.: zdarzenia klawiaturowe, ruchy kursora myszy, zdarzenia dotykowe na ekranach dotykowych, dane z czujników ruchu urządzenia (akcelerometr, żyroskop, magnetometr), wybrane dane kontekstowe (np. typ przeglądarki, system operacyjny, parametry sesji sieciowej).

Po stronie serwera funkcjonuje moduł odpowiedzialny za: przetwarzanie wstępne sygnału, ekstrakcję cech, ocenę ryzyka i detekcję anomalii przy użyciu algorytmów sztucznej inteligencji, generowanie decyzji (np. „kontynuuj", „zażądaj dodatkowego uwierzytelnienia", „zablokuj").

Taki podział minimalizuje obciążenie urządzenia klienta, ogranicza możliwość lokalnej manipulacji sygnałem przez złośliwe oprogramowanie oraz pozwala na centralne doskonalenie modeli analitycznych. Jednocześnie architektura ta dobrze wpisuje się w wymagania nadzorcze dotyczące zarządzania obszarami technologii informacyjnej (IT) oraz bezpieczeństwa środowiska teleinformatycznego formułowane przez Komisję Nadzoru Finansowego[147].

W praktyce systemy biometrii behawioralnej nie opierają się na pojedynczej cesze, lecz na fuzji wielowymiarowych sygnałów przetwarzanych w modelu uczenia maszynowego. Kluczowe znaczenie ma integracja danych motorycznych, temporalnych i kontekstowych, które łącznie budują probabilistyczny profil użytkownika. Mechanizmy klasyfikacyjne analizują nie tylko pojedyncze parametry (np. rytm pisania czy dynamikę gestów), lecz także ich współwystępowanie oraz odchylenia od wzorca referencyjnego w określonym kontekście operacyjnym. Włączenie sygnałów środowiskowych (np. charakterystyki urządzenia) oraz kontekstu transakcyjnego umożliwia zastosowanie podejścia *risk-based authentication*, w którym decyzja nie ma charakteru binarnego, lecz opiera się na ocenie poziomu ryzyka. Takie podejście prowadzi do poprawy jakości klasyfikacji oraz redukcji błędów typu fałszywa akceptacja i fałszywe odrzucenie, przy jednoczesnym ograniczeniu wpływu na doświadczenie użytkownika.

Gromadzenie danych na taką skalę wiąże się z konkretnymi wyzwaniami technicznymi i regulacyjnym (wskazane zostały w rozdziale 6). Wymiar regulacyjny tych wyzwań dotyczy przede wszystkim dopuszczalności i warunków przetwarzania danych biometrycznych jako danych osobowych. Kluczowa jest kwalifikacja danych i ustalenie podstawy prawnej przetwarzania, w tym rozstrzygnięcie, czy w danym modelu rozwiązanie zmierza do jednoznacznej identyfikacji osoby, czy ma charakter oceny ryzyka i wykrywania anomalii w sesji. Ponadto konieczne jest

144 Parlament Europejski i Rada (UE). Dyrektywa (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (PSD2). Dziennik Urzędowy UE L 337/35.

145 Teh, P. S., Zhang, N., Teoh, A. B. J., Chen, K. A survey on touch dynamics authentication in mobile devices. Computers & Security, vol. 59, 2016.

146 Stylios, I., Kokolakis, S., Thanou, O., Chatzis, S. Behavioral biometrics and continuous user authentication on mobile devices: a survey. Information Fusion, vol. 66, 2021.

147 https://www.knf.gov.pl/knf/pl/komponenty/img/knf_125701_PTE_Wytyczne_IT_16_12_2014_40005.pdf

wykazanie zasady minimalizacji i proporcjonalności, Wreszcie, w praktyce regulacyjnej szczególnego znaczenia nabiera obowiązek przeprowadzenia oceny skutków dla ochrony danych w sytuacjach, w których przetwarzanie może powodować wysokie ryzyko dla praw i wolności osób, zwłaszcza gdy ma ono charakter ciągły, obejmuje profilowanie zachowań i jest realizowane na dużą skalę. Podsumowując, przetwarzanie danych biometrycznych rodzi wymogi w zakresie przejrzystości i informowania, gdyż użytkownik powinien rozumieć, jakie kategorie danych są zbierane, w jakim celu, jak długo oraz jakie konsekwencje może wywołać wynik analizy, na przykład uruchomienie dodatkowego uwierzytelnienia albo wstrzymanie transakcji. Z uwagi na wykorzystanie modeli analitycznych pojawiają się wymogi dotyczące rozliczalności, testowania i nadzoru nad modelem, w tym zarządzania ryzykiem błędnych decyzji i potencjalnej stronniczości, ponieważ nierównomierna skuteczność wobec różnych urządzeń i sposobów korzystania z usług może prowadzić do nieproporcjonalnych obciążeń części użytkowników. Warto zaznaczyć, że znaczenie mają regulacje sektorowe dotyczące odporności operacyjnej i bezpieczeństwa IT, ponieważ bank musi wykazać adekwatność zabezpieczeń technicznych i organizacyjnych, kontrolę dostawców oraz odporność procesu na nadużycia i manipulacje.

4.2.2. Przetwarzanie wstępne, normalizacja i ekstrakcja cech

Surowe dane z urządzeń użytkownika nie nadają się bezpośrednio do modelowania – są zaszumione, nieregularne czasowo i zależne od charakterystyk sprzętu. Dlatego kluczowy etap stanowi przetwarzanie wstępne (*preprocessing*), normalizacja oraz inżynieria cech (*feature engineering*).

W fazie przetwarzania wstępnego typowo stosuje się: a) filtrowanie szumu (np. wygładzanie sygnałów, filtry cyfrowe) w celu usunięcia artefaktów sprzętowych; b) segmentację sygnału – dzielenie strumienia zdarzeń na logiczne jednostki (pojedyncze gesty, sesje wpisywania tekstu, epizody nawigacji); c) detekcję i usuwanie wartości odstających z wykorzystaniem algorytmów statystycznych lub nienadzorowanych metod ML; d) uzupełnianie braków danych (interpolacja, imputacja) w sytuacjach częściowej utraty sygnału.

Celem normalizacji jest oddzielenie właściwego sygnału behawioralnego od wpływu kontekstu (urządzenie, pora dnia, rodzaj interakcji). Stosuje się m.in.: normalizację zorientowaną na użytkownika (*user-specific*) – skalowanie cech względem typowych wartości dla danego klienta, tzw. normalizację globalną – odniesienie do parametrów populacji referencyjnej oraz normalizację świadomą kontekstu (*context-aware*) – odrębne modele dla typowych scenariuszy (np. aplikacja mobilna vs. bankowość internetowa). Badania nad ciągłym uwierzytelnianiem na urządzeniach mobilnych wskazują, że normalizacja kontekstowa istotnie redukuje liczbę fałszywych odrzuceń, szczególnie gdy użytkownik często zmienia tryb pracy lub urządzenia.

Po przetworzeniu wstępnym dane są przekształcane do wektorów cech, które mają maksymalizować separowalność pomiędzy użytkownikami przy zachowaniu stabilności w czasie:

- cechy czasowe – m.in. czasy naciśnięcia i zwolnienia klawisza, interwały między zdarzeniami, prędkości gestów;
- cechy przestrzenne – kształt trajektorii, krzywizna, rozkład punktów dotyku;
- cechy częstotliwościowe – wynik transformacji (np. transformacji Fouriera, falkowej) na sygnałach czasowo-przestrzennych;
- cechy kognitywne – opisujące sposób podejmowania decyzji (wahanie, powrót do poprzednich ekranów, nietypowe ścieżki nawigacji).

W nowoczesnych systemach coraz częściej odchodzi się od ręcznie projektowanych cech na rzecz reprezentacji uczonych automatycznie, z wykorzystaniem sieci konwolucyjnych CNN (*Convolutional Neural Network*) i rekurencyjnych RNN (*Recurrent Neural Network*), a także ich wariantów (np. *LSTM – Long Short-Term Memory, GRU – Gated Recurrent Unit*)[148].

148 Papaioannou, M., Mantas, G., Panaousis, E. M., Essop, A., Rodriguez, J., Sucasas, V. Behavioral Biometrics for Mobile User Authentication: Benefits and Limitations. 2023 IFIP Networking Conference (IFIP Networking).

4.2.3. Modelowanie, wnioskowanie i detekcja anomalii

We wczesnych pracach oraz w środowiskach o ograniczonych zasobach stosowano przede wszystkim klasyczne algorytmy uczenia maszynowego, takie jak modele regresyjne i drzewa decyzyjne, las losowy czy metody wektorów wspierających do detekcji anomalii na podstawie wzorca „normalnego" zachowania, metody *boostingowe* (np. XGBoost) dla złożonych, heterogenicznych zestawów cech.

Modele te są relatywnie proste obliczeniowo, łatwe do wyjaśnienia i dobrze sprawdzają się w systemach, w których ważna jest interpretowalność decyzji (np. pod kątem wymogów nadzorczych KNF i oczekiwań audytorów).

Dla złożonych, wielowymiarowych strumieni danych behawioralnych dominujące stają się jednak architektury DL (*Deep Learning*), w szczególności:

- RNN (ang. *Recurrent Neural Network*) oraz LSTM (ang. *Long Short-Term Memory*) – do modelowania sekwencji czasowych (rytmy pisania, serie gestów),
- Hybrydy: CNN (ang. *Convolutional Neural Network*) + RNN – do jednoczesnego wykorzystania informacji przestrzennej i czasowej,
- Autoenkodery (ang. *Autoencoders*) – jako modele nienadzorowane do wykrywania odchyleń od wzorca,
- Architektury oparte na mechanizmie uwagi (*Transformers*), zdolne do przetwarzania długich sekwencji i wielu kanałów sygnału.

Z punktu widzenia banku kluczowe jest nie tylko rozpoznanie użytkownika, ale przede wszystkim wykrycie zachowań anomalnych związanych z: przejęciem urządzenia lub sesji, działaniem złośliwego oprogramowania, atakami socjotechnicznymi, w których klient działa pod wpływem manipulacji, próbami odtworzenia zachowania przez atakującego (np. powtarzanie gestów).

W rozwiązaniach produkcyjnych stosuje się podejścia oparte na modelach jednoklasowych, gdzie modelowane jest wyłącznie „normalne" zachowanie klienta, a każde istotne odchylenie jest traktowane jako potencjalne zagrożenie. Wykorzystywane są także modele hybrydowe, łączące profil użytkownika z profilami typowych scenariuszy ataku.

W literaturze przedmiotu podkreśla się, że szczególnie skuteczne są rozwiązania, które traktują ciągłe uwierzytelnianie behawioralne jako element szerszej architektury „*risk-based authentication*", a nie jako pojedynczy mechanizm decyzyjny[149].

4.2.4. Fuzja

Systemy biometrii behawioralnej rzadko opierają się na pojedynczym rodzaju danych; kluczowe jest łączenie wielu modalności. Podejścia wielomodalne łączą m.in.: dynamikę klawiatury, dynamikę dotyku, dane z akcelerometru i żyroskopu, wzorce korzystania z aplikacji, sygnały lokalizacyjne i parametry sieciowe. Przykładowo, w literaturze[150] pokazano, że łączenie nawet siedmiu kanałów danych pozwala znacząco obniżyć EER w stosunku do systemów jednokanałowych.

Fuzja może być realizowana na różnych poziomach:

- fuzja na poziomie cech (*feature-level fusion*) – łączenie wektorów cech w jedną reprezentację;
- fuzja na poziomie decyzji (*score-level fusion*) – łączenie wyników kilku niezależnych klasyfikatorów;
- architektury hierarchiczne, w których np. decyzja wysokiego ryzyka uruchamia dodatkowe mechanizmy (np. jednorazowa dodatkowa SCA).

149 Mahfouz, A., Mahmoud, T. M., Sharaf Eldin, A. A Survey on Behavioral Biometric Authentication on Smartphones. Computers & Security, 2017.

150 Bo, C., Zhang, L., Li, X.-Y. SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics. CoRR abs/1309.0073, 2013.

4.2.5 Podsumowanie

W praktyce bankowej algorytmy biometrii behawioralnej są umieszczane w szerszym ekosystemie zarządzania ryzykiem, w którym wynik behawioralny jest jednym z wejść do silnika decyzyjnego – obok oceny ryzyka transakcyjnego, historii klienta oraz innych mechanizmów antyfraudowych[151].

W nowoczesnych systemach stosuje się zatem mechanizmy uczenia ciągłego, w których profil klienta jest stopniowo aktualizowany na podstawie kolejnych, prawidłowych sesji. Wdrożenie takich rozwiązań wymaga jedna zdefiniowania kryteriów, kiedy dana próbka może zostać włączona do wzorca oraz ograniczenia „szybkości zapominania" (ang. *forgetting rate*), aby profil nie stał się zbyt wrażliwy na krótkotrwałe zmiany, jak i wymaga mechanizmów detekcji nagłych zmian, które mogą sugerować przejęcie konta.

Profil behawioralny może być różny w zależności od kontekstu – inaczej użytkownik korzysta z bankowości webowej w pracy, inaczej z aplikacji mobilnej wieczorem. Badania wskazują, że budowa kilku profili częściowych (np. „mobile-on-the-go", „desktop-office") dla tego samego klienta poprawia dokładność w porównaniu z pojedynczym profilem globalnym. Takie podejście jest zgodne z koncepcją uwierzytelniania ciągłego, w której system nie tylko odpowiada na pytanie „kim jest użytkownik? ", ale również „czy jego aktualne zachowanie jest spójne z oczekiwanym wzorcem w danym kontekście? ".

4.3. Zastosowania w procesie KYC (*Know Your Customer*) i ciągłym monitoringu użytkownika

Tradycyjne procedury KYC (*Know Your Customer*) koncentrują się na identyfikacji i weryfikacji klienta na etapie nawiązania relacji oraz na okresowej aktualizacji danych zgodnie z wymogami AML/CFT. Model ten ma charakter punktowy – zakłada, że tożsamość klienta została ustalona w momencie onboardingu, a dalsza relacja opiera się na przyjęciu jej względnej stabilności[152]. W praktyce jednak ryzyko nadużyć nie jest zdarzeniem jednorazowym, lecz procesem dynamicznym. Przejęcie rachunku, wykorzystanie tożsamości przez osobę trzecią czy stopniowa zmiana profilu aktywności mogą wystąpić długo po zakończeniu procedury weryfikacyjnej. Z tego względu w literaturze i praktyce nadzorczej coraz częściej pojawia się koncepcja tzw. „ciągłego KYC" (*continuous KYC*), rozumianego jako bieżąca ocena ryzyka klienta w trakcie trwania relacji, a nie wyłącznie na jej początku.

Biometria behawioralna może stanowić techniczne wsparcie takiego podejścia. Nie zastępuje ona klasycznych wymogów identyfikacyjnych, lecz uzupełnia je o warstwę monitorowania zgodności zachowania z ustalonym profilem ryzyka. W tym ujęciu analiza wzorców interakcji przestaje pełnić wyłącznie funkcję uwierzytelniającą, a staje się elementem systemu zarządzania ryzykiem operacyjnym i przeciwdziałania nadużyciom[153].

Należy przy tym wyraźnie odróżnić *continuous KYC* od formalnego silnego uwierzytelnienia klienta (SCA) w rozumieniu PSD2. O ile SCA ma charakter transakcyjny i punktowy, o tyle analiza behawioralna może funkcjonować jako mechanizm wspierający ocenę ryzyka w trakcie całej relacji z klientem. W praktyce oznacza to ciągłe, pasywne monitorowanie charakterystycznych wzorców interakcji użytkownika z urządzeniami i aplikacjami (np. rytmu pisania, dynamiki gestów czy sposobu korzystania z interfejsu). Na tej podstawie budowany jest indywidualny profil zachowań, który może być wykorzystywany do wykrywania odchyleń od normy w trakcie sesji. W odróżnieniu od biometrii fizycznej, cechy behawioralne mają charakter dynamiczny, co utrudnia ich skuteczne odwzorowanie bez pozostawienia wykrywalnych anomalii. Dzięki temu uwierzytelnianie behawioralne może pełnić rolę niewidocznej, ciągłej warstwy bezpieczeństwa – także w sytuacji, gdy atakujący pozyska statyczne dane uwierzytelniające[154].

W praktyce zastosowanie biometrii behawioralnej w procesach instytucji finansowych dotyczy przede wszystkim wykrywania nadużyć (*fraud detection*),

151 European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape: Finance Sector – January 2023 to June 2024, 2025. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf.

152 Rajdev, R., From KYC to KYCB: Moving Towards Behavioral Compliance in Digital Finance, SSRN Preprint, 2025.

153 Feedzai, What Is Behavioral Biometrics and How Does It Work Against Fraud?, 2024.

154 Obiektywne Finanse, Biometria behawioralna w polskich bankach, 2024.

a nie klasycznej identyfikacji KYC sensu stricto. O ile procedury AML koncentrują się na analizie przepływów finansowych i wzorców transakcyjnych, o tyle biometria behawioralna pozwala ocenić, czy sposób korzystania z systemu jest zgodny z profilem danego użytkownika. Systemy te dostarczają tzw. sygnałów pasywnych, takich jak sposób wypełniania formularzy, dynamika nawigacji czy wzorce interakcji z interfejsem. Analiza tych metadanych umożliwia wykrywanie prób przejęcia tożsamości, automatyzacji procesów (botów) lub składania wniosków przy użyciu cudzych danych. Przykładowo nienaturalnie szybkie, zautomatyzowane uzupełnianie formularzy przy jednoczesnym braku typowych dla użytkownika wahań może wskazywać na działanie skryptu lub osoby trzeciej. W takim ujęciu warstwa behawioralna wspiera przede wszystkim systemy przeciwdziałania oszustwom oraz ochrony przed przejęciem rachunku, natomiast jej rola w klasycznym monitoringu AML ma charakter pośredni i ograniczony[155]. Włączenie analizy zachowania do procesów bezpieczeństwa stanowi zatem uzupełnienie tradycyjnych metod identyfikacji i monitoringu transakcyjnego, a nie ich zastąpienie.

Na dalszych etapach relacji z klientem biometria behawioralna znajduje zastosowanie przede wszystkim w obszarze przeciwdziałania nadużyciom (*anti-fraud*) oraz ochrony przed przejęciem rachunku (*Account Takeover – ATO*). Wspiera ona mechanizmy ciągłego uwierzytelniania oraz monitorowania sesji użytkownika. Każda sesja bankowości internetowej lub mobilnej może być na bieżąco oceniana pod kątem zgodności z typowym profilem zachowań danego klienta. Algorytmy działające w czasie rzeczywistym pozwalają identyfikować sygnały wskazujące na zagrożenie, takie jak oznaki automatyzacji, symptomy zdalnej kontroli urządzenia czy istotne odchylenia od dotychczasowych wzorców interakcji. Szczególne znaczenie ma to w przypadkach oszustw socjotechnicznych, gdy uprawniony klient działa pod wpływem manipulacji. W takich sytuacjach mogą pojawiać się mierzalne zmiany w dynamice korzystania z systemu (np. zwiększone wahania czasowe, nietypowe sekwencje działań czy nagłe zmiany tempa interakcji). Warstwa behawioralna może wówczas zainicjować dodatkową weryfikację lub podwyższony poziom autoryzacji przed realizacją transakcji. Mechanizmy te należy traktować jako element systemów przeciwdziałania oszustwom i zarządzania ryzykiem operacyjnym, a nie jako narzędzie realizacji obowiązków KYC lub klasycznego monitoringu AML[156].

Integracja biometrii behawioralnej z architekturą bezpieczeństwa banku umożliwia realizację podejścia *risk-based authentication*, czyli uwierzytelniania adaptacyjnego opartego na bieżącej ocenie ryzyka. W większości przypadków sesje klientów mogą przebiegać bez dodatkowych barier, a system pozostaje niewidoczny, dopóki zachowanie użytkownika mieści się w przyjętych normach. W sytuacji wykrycia istotnych odchyleń następuje automatyczne podniesienie poziomu zabezpieczeń, np. poprzez żądanie dodatkowego uwierzytelnienia lub czasowe wstrzymanie transakcji. Takie podejście pozwala pogodzić wysoki poziom ochrony z wygodą użytkownika. Przykłady wdrożeń pokazują, że jedynie niewielki odsetek podejrzanych logowań wymaga zastosowania dodatkowych mechanizmów, podczas gdy większość klientów korzysta z bankowości w sposób niezakłócony[157].

Podsumowując, wykorzystanie biometrii behawioralnej w procesach KYC i ciągłego monitorowania znacząco poszerza zakres „poznania klienta" przez instytucję finansową. Bank nie ogranicza się wyłącznie do potwierdzenia tożsamości na podstawie dokumentów, lecz jest w stanie ocenić, czy z konta faktycznie korzysta właściwa osoba i czy jej zachowanie pozostaje spójne z dotychczasowym profilem. Technologia ta działa w tle, bez angażowania użytkownika, a jednocześnie dostarcza wartościowych danych kontekstowych dla systemów antyfraudowych. W warunkach rosnącej skali ataków, takich jak przejęcia kont, phishing czy oszustwa przy zakładaniu rachunków, biometria behawioralna staje się ważnym elementem proaktywnej strategii bezpieczeństwa. W efekcie biometria behawioralna przesuwa podejście KYC na wyższy poziom dojrzałości: od jednorazowej identyfikacji do ciągłego potwierdzania, że klient pozostaje sobą podczas każdej interakcji z usługą bankową.

155 BioCatch, Digital Bank Account Opening Case Study – Behavioral Biometrics Prevents Massive New Account Opening Fraud Attack, 2021.

156 Behavioural Biometrics and Device Intelligence in Fraud Strategies.

157 ThreatMark, How AI-Powered Authentication Enhances Security & UX for Slovenská sporiteľňa, case study, 2022.

4.4. Studia przypadków – wdrożenia w sektorze finansowym

Biometria behawioralna w ciągu ostatnich lat przeszła drogę od technologii eksperymentalnej do realnie wdrażanej w instytucjach finansowych na całym świecie. Wiele banków i firm fintech dostrzegło jej potencjał zarówno w zwiększaniu bezpieczeństwa, jak i poprawie wygody klientów. Poniżej przedstawiono wybrane *studia przypadków* obrazujące praktyczne efekty implementacji w sektorze finansowym.

Jednym z głośnych przykładów zastosowania analizy behawioralnej jest ochrona procesu otwierania rachunków online. Nowe banki cyfrowe, dążąc do szybkiego wzrostu bazy klientów, często padają ofiarą masowych ataków polegających na tworzeniu fikcyjnych kont przy użyciu skradzionych lub syntetycznych tożsamości. Przykładem instytucji finansowej, wobec której organ nadzoru wskazał istotne uchybienia w obszarze kontroli przestępczości finansowej obejmujące procesy przyjmowania klientów i weryfikacji danych, jest Monzo Bank Ltd., ukarany[158] przez **FCA** w 2025 r. Tradycyjne metody weryfikacji (skany dokumentów, baza PESEL itp.) mogą nie wychwycić znakomicie podrobionych danych osobowych, zwłaszcza jeśli pochodzą z prawdziwych wycieków. Biometria behawioralna dodaje tu *kolejną linię obrony*: analizuje sposób wypełniania wniosku i interakcji z formularzem przez rzekomego nowego klienta. BioCatch, jeden z liderów w tej dziedzinie, opublikował opis incydentu[159], w którym *digital bank* stał się celem zorganizowanej grupy przestępczej podczas kampanii promocyjnej nowych kont. Atak polegał na zakładaniu setek kont przez oszustów w celu wyłudzenia premii powitalnych i ułatwienia kradzieży środków. Wdrożony system behawioralny wykrył tę nietypową aktywność w czasie rzeczywistym, analizując m.in. płynność nawigacji (oszuści wykazywali *nienaturalną biegłość* – przeskakiwali pola formularza w ustalonym rytmie, nie czytając podpowiedzi) oraz znajomość danych (schemat wprowadzania informacji sugerujący korzystanie z listy danych ofiar). Dzięki alertom behawioralnym bank zablokował fale fałszywych wniosków, podnosząc wskaźnik wykrywania fraudów o 60% powyżej dotychczasowych metod (urządzenie, geolokalizacja, czarne listy). Ta skuteczna obrona pozwoliła bankowi bezpiecznie kontynuować akwizycję klientów – jak podano, w szczytowym momencie ataku system BioCatch identyfikował charakterystyczne wzorce przestępców z ponad *70% skutecznością wyższą* niż poprzednie reguły, co umożliwiło uniknięcie milionowych strat. Case study to pokazuje, że dla procesu KYC przy otwieraniu kont dodanie analizy behawioralnej znacząco uszczelnia system – pozwalając rozróżnić prawdziwych klientów od zautomatyzowanych wniosków czy osób podszywających się pod innych.

Kolejnym obszarem wdrożeń są klasyczne systemy transakcyjne banków – bankowość internetowa i aplikacje mobilne – gdzie biometria behawioralna pełni funkcję „strażnika sesji". Przykładem jest tu zastosowanie platformy behawioralnej w bankach europejskich do zwalczania przejęć kont (ATO) i oszustw typu social engineering (np. scam na policjanta, fałszywy konsultant banku)[160].

Na szczególną uwagę zasługuje doświadczenie banków, które zastosowały biometrię behawioralną do spełnienia wymogów PSD2 w zakresie tzw. silnego uwierzytelniania klienta w sposób przyjazny dla klienta. Grupa Erste wdrożyła platformę ThreatMark Behavioral Intelligence jako element systemu transakcyjnego i raportuje szereg korzyści. Po pierwsze, zredukowano o ponad połowę średni czas spędzany przez klienta na stronie logowania, ponieważ mniej dodatkowych kroków było wymaganych[161]. Po drugie, dzięki adaptacyjnemu podejściu (behawioralna ocena ryzyka) tylko ~10% logowań i transakcji wymagało silniejszego uwierzytelnienia (reszta była na tyle „bezpieczna behawioralnie", że nie było to potrzebne). Po trzecie, bank odnotował 90% spadek liczby fałszywych alarmów w systemie antyfraudowym – analiza behawioralna dostarcza bowiem dodatkowego kontekstu, pozwalając odfiltrować nieszkodliwe odstępstwa od normy od faktycznych zagrożeń. Co kryje się za tymi liczbami, to realne oszczędności: bank oszacował, że zaoszczędził ok. 1 mln € rocznie na kosztach SMS-ów autoryzacyjnych i obsłudze alertów, które wcześniej były generowane zbyt często. Przykład ten dowodzi, że biometria behawioralna może skutecznie zrównoważyć bezpieczeństwo i wygodę – spełniając rygorystyczne wymogi regulacyjne (SCA) i jednocześnie upraszczając użytkownikom życie (mniej haseł jednorazowych, mniej frustracji).

Polska bankowość cyfrowa jest pionierem we wprowadzaniu biometrii behawioralnej na skalę między-

158 https://www.fca.org.uk/publication/final-notices/monzo-bank-limited.pdf.

159 https://www.biocatch.com/hubfs/Case_Studies/Digital%20Bank%20Account%20Opening%20Case%20Study(1).pdf.

160 https://www.biocatch.com/hubfs/Case_Studies/Biocatch_CS_ATO_Journey%202020%20-%20v4.pdf

161 ThreatMark, How AI-Powered Authentication Enhances Security & UX for Slovenská sporiteľňa, case study, 2022.

bankową. W 2023 r. Biuro Informacji Kredytowej (BIK) uruchomiło Sektorową Platformę Biometrii Behawioralnej – rozwiązanie dostępne dla całego sektora finansowego w Polsce, umożliwiające współdzielenie sygnałów behawioralnych między instytucjami. Celem jest zbudowanie *sieci wczesnego ostrzegania*: jeżeli w Banku A wykryto oszukańcze zachowanie na koncie klienta, informacja (anonimowa w kontekście danych osobowych, ale znacząca behawioralnie) może zostać wykorzystana przez Bank B, zanim ten padnie ofiarą tego samego oszusta. Takie międzybankowe podejście pozwala również rozwiązać problem *„zimnego startu"* – gdy nowy klient nie ma historii zachowań w danym banku, można odwołać się do jego profilu zbudowanego w innej instytucji (za zgodą klienta). Według komunikatów BIK[162], Polska jest jednym z pierwszych rynków na świecie, gdzie wdrożono tego typu sektorową współpracę w obszarze analizy behawioralnej.

Pierwsze wdrożenia w ramach Platformy BIK nastąpiły w latach 2023–2024: ING Bank Śląski jako pierwszy włączył usługę *weryfikacji behawioralnej* do swojego systemu transakcyjnego już pod koniec 2023 r., a w 2024 r. dołączyły BNP Paribas Bank Polska oraz VeloBank. Kolejne instytucje finalizują integrację – np. Bank Pekao S.A. zaplanował uruchomienie systemu w połowie 2025 r., a największa kasa oszczędnościowa (SKOK Stefczyka) – pod koniec 2024 r.[163] Warto dodać, że równolegle *niektóre banki zdecydowały się na własne implementacje* poza platformą BIK: Credit Agricole Polska wdrożył mechanizmy behawioralne (we współpracy z Digital Fingerprints) niezależnie, uruchamiając je dla bankowości internetowej i mobilnej na początku 2025 roku. Już wcześniej, bo w 2018 r., mBank przeprowadził pilotaż biometrii behawioralnej, również we współpracy z Digital Fingerprints, co czyni go jednym z prekursorów tych rozwiązań.

Efekty wdrożeń w polskim sektorze potwierdzają wysoką skuteczność technologii. ING Bank Śląski ujawnił[164], że wśród klientów, którzy padli ofiarą oszustw, odsetek osób z aktywowaną biometrią behawioralną był poniżej 4%, a w niektórych okresach spadał nawet poniżej 1%. Innymi słowy, przytłaczająca większość fraudów dotyczyła klientów, którzy nie mieli włączonej ochrony behawioralnej, co wskazuje na realną redukcję ryzyka dzięki temu mechanizmowi. Banki podkreślają też korzyści miękkie: zwiększenie zaufania klientów oraz poprawę ich poczucia bezpieczeństwa.

Wdrożenia biometrii behawioralnej w sektorze finansowym pokazują, że technologia ta przynosi wymierne korzyści: zwiększa wykrywalność ataków i nadużyć, zmniejsza straty finansowe banków (zarówno bezpośrednie, jak i pośrednie koszty obsługi fraudów), a zarazem poprawia doświadczenie klientów przez ograniczenie niepotrzebnych utrudnień. Banki korzystające z tych systemów odnotowały spadek wskaźnika fałszywych alarmów, co sugeruje, że decyzje o blokadach są podejmowane precyzyjniej – tylko wtedy, gdy rzeczywiście dzieje się coś podejrzanego. To z kolei przekłada się na mniejsze obciążenie call center i działów obsługi reklamacji, bo klienci rzadziej zgłaszają zablokowanie niesłusznie swoich transakcji czy kont. Jednocześnie rośnie skuteczność wykrywania nowych, bardziej wyrafinowanych zagrożeń, takich jak oszustwa socjotechniczne w czasie rzeczywistym. Dzięki analizie zachowania możliwe jest wykrycie, że *użytkownik pada ofiarą manipulacji w trakcie trwania transakcji* – co klasyczne systemy (typu *rule-based*) często nie potrafią, gdyż koncentrują się na parametrach transakcji, a nie sposobie działania użytkownika.

Warto podkreślić, że wdrażanie biometrii behawioralnej zbiega się z globalnymi trendami i rekomendacjami. Analiza raporty opracowanego przez ENISA[165] wskazuje sektor bankowy, jako taki, który musi adaptować rozwiązania AI do walki z nowymi formami cyberzagrożeń, a rynek rozwiązań behawioralnych dynamicznie rośnie.

Biometria behawioralna pomaga bankom wykazać zgodność z wymogami *Strong Customer Authentication* bez pogarszania UX, a także wpisuje się w koncepcję tzw. *„perpetual KYC"* (ciągłego poznawania klienta) zalecaną w nowoczesnych ramach AML[166].

162 https://rozwiazania-antyfraudowe.bik.pl/pl/platforma-weryfikacji-behawioralnej.

163 Obiektywne Finanse, Biometria behawioralna w polskich bankach, 2024.

164 https://www.cashless.pl/14353-ing-biometria-behawioralna-statystyki.

165 https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf.

166 Vacuumlabs, Guide: What is KYC in Banking (Challenges and Future), 2023.

Rozdział 5. Biometria behawioralna a cyberbezpieczeństwo banku

5.1. Rola w zapobieganiu oszustwom i nadużyciom (*fraud detection*)

W obliczu rosnącej skali oszustw w bankowości cyfrowej tradycyjne zabezpieczenia okazują się niewystarczające. Współczesne podejście do bezpieczeństwa odchodzi od jednorazowej weryfikacji tożsamości na rzecz ciągłej oceny ryzyka w czasie rzeczywistym.

Przypomnijmy: mechanizm działania biometrii behawioralnej polega na zbieraniu w trakcie sesji setek mikrosygnałów dotyczących interakcji użytkownika z interfejsem. Po stronie klienta (przeglądarki lub aplikacji mobilnej) rejestrowane są m.in. zdarzenia klawiatury, ruchy kursora myszy, dotknięcia ekranu dotykowego oraz dane z czujników ruchu urządzenia (akcelerometr, żyroskop). Dane te przesyłane są bezpiecznie do centralnego silnika analitycznego, gdzie poddaje się je wstępnemu przetwarzaniu, ekstrakcji cech i analizie z wykorzystaniem algorytmów AI/ML. Model behawioralny buduje profil odniesienia charakterystyczny dla danego użytkownika, obejmujący cechy motoryczne i kognitywne. Podczas każdej kolejnej aktywności system porównuje nowe dane z profilem wzorcowym i oblicza ryzyko anomalii. W praktyce decyzje podejmowane są w ułamkach sekund – jeśli zachowanie odbiega od normy, generowany jest odpowiedni alert lub podejmowana jest akcja (np. wymuszenie dodatkowej weryfikacji lub zablokowanie operacji). Taki podział architektury (lekki klient, ciężka analityka po stronie serwera) zapewnia zarówno skuteczność, jak i bezpieczeństwo – modele mogą być ciągle doskonalone centralnie, a obciążenie urządzeń użytkowników pozostaje minimalne. Co istotne, profil behawioralny adaptuje się w czasie do naturalnych zmian w zachowaniu użytkownika, aby ograniczyć ryzyko fałszywych odrzuceń (FRR) wynikających ze sztywnego wzorca.

Przejęcie konta bankowego przez oszusta z użyciem prawidłowych poświadczeń uwierzytelniających (np. login, hasło, przechwycony kod SMS) należy do najpoważniejszych zagrożeń współczesnej bankowości. W takim scenariuszu tradycyjny system uznaje logowanie za legalne – dopiero analiza behawioralna pozwala zajrzeć „pod powierzchnię" i odróżnić legalnego użytkownika od intruza. Oszust (działający interaktywnie lub automatycznie) zdradza się nietypowym sposobem korzystania z systemu: porusza się szybciej i bardziej schematycznie, pomijając standardowe elementy nawigacji (np. nie sprawdza salda, od razu przechodzi do formularza przelewu), często używa techniki *copy–paste* do wprowadzania danych (podczas gdy właściciel konta zwykle wpisuje je ręcznie) i wykonuje w krótkim czasie serię transakcji, przekraczającą normalne przyzwyczajenia użytkownika. Jednocześnie może ujawniać oznaki nieludzkiej automatyzacji – boty wykazują *nadludzką szybkość* wpisywania danych oraz nienaturalnie równy rytm klikania, pozbawiony ludzkich wahań i błędów. Ataki zdalne z użyciem narzędzi typu RAT również pozostawiają ślady behawioralne: kursory poruszają się skokowo wskutek opóźnień sieciowych, a na urządzeniu mobilnym brak fizycznych dotknięć ekranu mimo aktywności interfejsu (sygnał przejęcia sesji). System wychwytuje także próby emulacji urządzenia – generowanie idealnie powtarzalnych, „zbyt doskonałych" ruchów kursora czy nacisków dotykowych, niemożliwych dla ludzkiej ręki. Dzięki korelacji wielu takich cech, algorytmy behawioralne potrafią z wysokim prawdopodobieństwem rozpoznać, że za klawiaturą siedzi ktoś inny niż deklarowany klient. Bank może w ułamku sekundy przerwać podejrzaną sesję lub zażądać dodatkowej weryfikacji tożsamości, zapobiegając wyprowadzeniu środków. Instytucje finansowe, które konsekwentnie wykorzystują to podejście, raportują znaczące spadki liczby udanych przejęć kont po pełnym wdrożeniu technologii behawioralnej.

Coraz większy odsetek fraudów stanowią ataki, w których to sam użytkownik – będąc pod wpływem manipulacji – nieświadomie pomaga przestępcom. Kategoria ta obejmuje m.in. phishing (wyłudzanie poufnych informacji) oraz oszustwa typu *Authorized Push Payment*, gdzie ofiara nakłoniona przez cyberprzestępcę sama autoryzuje przelew na rachunek oszusta. Według danych UK Finance straty brytyjskich banków z tytułu fraudów APP sięgają ~460 mln funtów rocznie, co obrazuje skalę problemu[167]. Klasyczne mechanizmy uwierzytelniania (hasła, kody SMS) zawodzą tu, gdyż transakcję inicjuje prawidłowo zalogowany klient. Biometria behawioralna tworzy jednak dodatkową linię obrony poprzez analizę emocjonalno-poznawczych wskazówek, które mogą świadczyć o tym, że użytkownik działa pod przymu-

167 https://www.reuters.com/world/uk/uk-regulator-proposes-slashing-bank-reimbursement-cap-fraud-victims-2024-09-04.

sem lub jest zdalnie instruowany. System poszukuje tzw. *„cyfrowych tików”*, tj. subtelnych odchyleń od typowego stylu obsługi, mogących wskazywać na stres, dezorientację bądź coaching przez oszusta. Przykładowo, ofiary instruowane telefonicznie często wykazują segmentację pisania – wpisują dane partiami, z nienaturalnie długimi pauzami między kolejnymi fragmentami tekstu, odpowiadającymi rytmowi dyktowania przez kogoś w słuchawce. Pod presją zauważalne jest również wahanie kursora – użytkownik zawiesza kursor nad przyciskiem “Wyślij” dłużej niż zwykle, jakby potrzebował dodatkowej chwili na potwierdzenie decyzji. Czynniki motoryczne także odgrywają rolę: analiza danych z akcelerometru może ujawnić nietypowe drżenie ręki lub fakt, że telefon jest odkładany i podnoszony wielokrotnie w trakcie sesji – zachowania sugerujące zdenerwowanie lub konsultowanie się z kimś przed wykonaniem każdego kroku. Ponadto, długość trwania i liczba kroków w takiej sesji bywa większa niż normalnie (ofierze zabiera więcej czasu realizacja transakcji, bo kieruje się instrukcjami oszusta). Gdy system wykryje podobne anomalie świadczące o możliwym przymusie, może natychmiast podnieść poziom ryzyka i zażądać dodatkowego potwierdzenia tożsamości albo przerwać transakcję. Szczególne rezultaty osiągnięto łącząc sygnały behawioralne z innymi źródłami – np. kontekstem wielokanałowym. Jeżeli jednocześnie wykryto, że użytkownik w trakcie bankowania prowadzi rozmowę telefoniczną z nieznanym numerem i zleca przy tym przelew na nowego odbiorcę o wysokiej kwocie, system może automatycznie oznaczyć taką sytuację jako wysoce podejrzaną. Takie korelacje międzykanałowe zwiększają skuteczność wykrywania zaawansowanych oszustw, które pojedynczo nie dają się odróżnić od rutynowych działań.

Tradycyjne systemy antyfraudowe opierają się często na z góry zdefiniowanych regułach (np. „zablokuj przelew powyżej X, jeśli odbiorca jest nowy”) lub na modelach analitycznych uczonych na historycznych przypadkach nadużyć. Współczesne rozwiązania coraz częściej wykorzystują techniki uczenia maszynowego (machine learning – ML), które pozwalają identyfikować złożone wzorce ryzyka na podstawie dużych zbiorów danych. Choć metody te pozostają ważnym elementem ekosystemu bezpieczeństwa, mają istotne ograniczenia – reguły są sztywne i generują wiele fałszywych alarmów, a modele uczone wyłącznie na danych historycznych mogą nie nadążać za pojawieniem się nowych wektorów ataku oraz rzadkich zdarzeń charakterystycznych dla konkretnego użytkownika. Biometria behawioralna różni się od nich tym, że koncentruje się na sposobie wykonywania czynności (jak użytkownik działa), a nie wyłącznie na jej parametrach transakcyjnych (co robi). Dzięki temu możliwe jest wykrycie nieprawidłowości nawet wtedy, gdy pozostałe atrybuty transakcji (kwota, lokalizacja, urządzenie) mieszczą się w dopuszczalnym zakresie[168]. W praktyce rozwiązania behawioralne wykorzystują hybrydowe podejście łączące różne techniki analityczne. Obejmują one m.in. modele nadzorowane (uczone na oznaczonych przypadkach fraudów), metody wykrywania anomalii względem indywidualnego profilu użytkownika oraz algorytmy sekwencyjne analizujące ciągi zdarzeń w czasie. W bardziej zaawansowanych rozwiązaniach stosuje się także sieci neuronowe do identyfikacji złożonych wzorców ruchu czy trajektorii kursora oraz techniki łączenia wielu modeli (tzw. model fusion), które integrują sygnały behawioralne z kontekstem transakcyjnym i technicznym. Takie podejście zwiększa odporność systemu na próby obejścia zabezpieczeń i pozwala ograniczyć liczbę fałszywych alarmów w porównaniu z rozwiązaniami opartymi wyłącznie na prostych regułach decyzyjnych. W praktyce bankowej wynik analizy behawioralnej stanowi jeden z elementów szerszego silnika decyzyjnego zarządzania ryzykiem – obok oceny samej transakcji, reputacji urządzenia czy historii relacji z klientem. Biometria behawioralna uzupełnia więc istniejące mechanizmy, dostarczając dodatkowej warstwy sygnałów, zamiast je zastępować.

Na rynku istnieje już wiele dojrzałych rozwiązań z zakresu biometrii behawioralnej, a banki na całym świecie odnotowują dzięki nim wymierne korzyści. BioCatch – jeden z pionierów tej branży – dostarcza swoje systemy m.in. bankom w Wielkiej Brytanii, USA i Australii. Jego technologia koncentruje się na „profilowaniu poznawczym” użytkowników, pozwalając wykrywać tak subtelne zjawiska jak manipulacja ofiary przez oszusta (np. poprzez wychwytywanie opisanych wyżej wzorców segmentacji wpisywania danych czy nietypowego zawieszenia kursora). BehavioSec (obecnie część LexisNexis Risk Solutions)[169] specjalizuje się w dynamice klawiatury i interakcji użytkownika, oferując ciągłe uwierzytelnianie zarówno w kanałach web, jak i mobile – z jej rozwiązań korzystały m.in. banki skandynawskie oraz amerykańskie instytucje finansowe. Europejski dostawca ThreatMark (Czechy) z kolei integruje biometrię behawioralną z analizą szkodliwego oprogramowania i urządzeń, kładąc duży nacisk na pełne profilowa-

168 Behavioral Biometrics: What Is It & How It Works Against Fraud – SEON https://seon.io/resources/behavioral-biometrics-against-fraud/.

169 https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.1/risk-based-alerting/risk-scoring-in-splunk-enterprise-security.

nie sesji (od momentu logowania po zakończenie) oraz minimalizację *false positives*. Jego rozwiązania są popularne w regionie Europy Środkowo-Wschodniej, w tym we wdrożeniach bankowych w Polsce. Warto wspomnieć, że polski sektor bankowy wykazuje duże zainteresowanie tą technologią – już kilka lat temu PKO BP testował moduł dynamiki pisania podczas logowania, a ING Bank Śląski prowadził pilotaż ciągłego uwierzytelniania behawioralnego w aplikacji mobilnej. Globalnie rynek biometrii behawioralnej dynamicznie rośnie – szacuje się, że w skali roku o ok. 20%, przy czym to właśnie sektor finansowy jest największym odbiorcą tych rozwiązań. Studia przypadków publikowane przez dostawców regularnie pokazują redukcję fraudów typu ATO o ponad 50% po wdrożeniu biometrii behawioralnej[170], a jednocześnie poprawę satysfakcji użytkowników dzięki mniejszej liczbie uciążliwych procedur dodatkowej weryfikacji. Przykładowo, brytyjski bank NatWest we współpracy z Visa zastosował biometrię behawioralną podczas płatności online jako element wymogu *PSD2 Strong Customer Authentication (SCA)* – regulator uznał tę metodę za spełniającą kryterium *„coś, czym użytkownik jest/jak się zachowuje"* (czynnik inherence). Dzięki temu bank może zabezpieczać transakcje bez każdorazowego żądania od klienta dodatkowych haseł czy kodów SMS, co znacząco poprawia wygodę użytkowników. W dłuższej perspektywie NatWest sygnalizuje możliwość całkowitego odejścia od tradycyjnych haseł właśnie na rzecz uwierzytelniania behawioralnego działającego w tle. Również organizacja Visa[171] po udanych pilotażach udostępniła usługę analizy behawioralnej w ramach swojego systemu 3-D Secure (*Visa Behavioral Biometrics w VCAS*), co – według komunikatów Visa – przełożyło się na odczuwalne spadki fraudów oraz liczby fałszywych odrzuceń transakcji przy zakupach online. Te realne przykłady potwierdzają, że biometria behawioralna stała się ważnym elementem strategii cyberbezpieczeństwa banków, dostarczając nowego typu „inteligencji" o użytkowniku. Dzięki niej banki mogą lepiej równoważyć bezpieczeństwo z wygodą – wpisując się w paradygmat Zero Trust i ciągłego uwierzytelniania, gdzie tożsamość użytkownika jest weryfikowana nieustannie na podstawie *jak* się zachowuje, a nie tylko *kim* jest.

5.2. Integracja z systemami wykrywania anomalii i SIEM

Skuteczne wykorzystanie biometrii behawioralnej wymaga osadzenia jej w szerszym ekosystemie bezpieczeństwa banku. Dane dotyczące zachowania użytkowników nabierają realnej wartości dopiero wtedy, gdy są zestawiane z innymi zdarzeniami i alertami pochodzącymi z systemów monitoringu bezpieczeństwa. Z tego względu współczesne wdrożenia coraz częściej zakładają integrację silników analizy behawioralnej z platformami klasy SIEM (*Security Information and Event Management*) oraz narzędziami analizy zachowań użytkowników i innych elementów infrastruktury (*UEBA – User and Entity Behavior Analytics*), gdzie *„entity"* obejmuje m.in. urządzenia, konta techniczne czy systemy informatyczne[172]. Takie podejście umożliwia powiązanie anomalii behawioralnych z innymi sygnałami potencjalnego zagrożenia, na przykład nietypowym ruchem sieciowym, zmianą urządzenia czy lokalizacji logowania.

W rezultacie decyzje bezpieczeństwa mogą być podejmowane w sposób bardziej kontekstowy i dynamiczny. Przy niskim poziomie ryzyka system może ograniczyć ingerencję w doświadczenie użytkownika i nie wymagać dodatkowych kroków weryfikacyjnych, natomiast w przypadku wykrycia istotnych odchyleń od normy może zastosować środki podwyższonej kontroli, takie jak dodatkowe uwierzytelnienie czy czasowe wstrzymanie operacji. Takie podejście wpisuje się w założenia architektury Zero Trust, zgodnie z którą zaufanie nie jest przyznawane jednorazowo, lecz podlega ciągłej weryfikacji w trakcie trwania sesji. W praktyce wykrycie anomalii behawioralnej może zostać automatycznie powiązane z mechanizmami reagowania na incydenty funkcjonującymi w środowisku bezpieczeństwa banku. Integracja systemów analitycznych z platformami zarządzania zdarzeniami i reagowania umożliwia spójną oraz szybką reakcję – od podwyższenia poziomu uwierzytelnienia po przekazanie zdarzenia do dalszej analizy przez zespół bezpieczeństwa. Automatyzacja reakcji pozwala skrócić czas odpowiedzi na potencjalne zagrożenia, ograniczyć obciążenie operacyjne oraz zapewnić jednolite stosowanie polityk bezpieczeństwa w różnych kanałach dostępu.

Integracja systemów biometrii behawioralnej z platformami SIEM może być realizowana na różne sposoby, w zależności od architektury IT banku oraz możliwości oferowanych przez dostawcę rozwiązania. Najczęściej spotykane modele obejmują: (a) bez-

170 https://www.finextra.com/newsarticle/36008/natwest-tests-behavioural-biometrics-for-strong-customer-authentication.

171 https://www.visaitalia.com/content/dam/VCOM/regional/ve/unitedkingdom/PDF/sca/psd2-sca-challenge-design-best-practice-guide.pdf.

172 Adopt Behavioral Biometrics and Analytics for Effective Cybersecurity and Fraud Management.

pośrednie wykorzystanie API analitycznego, w ramach którego backend banku lub moduł pośredni pobiera bieżący wynik ryzyka dla danej sesji i przekazuje go do SIEM jako atrybut zdarzenia; (b) strumieniowe przesyłanie zdarzeń, gdzie silnik behawioralny publikuje informacje o wykrytych anomaliach do kolejki (np. Kafka) lub przesyła je protokołem syslog do konektora SIEM; (c) integrację opartą na logach, polegającą na okresowym importowaniu danych z systemu behawioralnego do SIEM w celu analizy i korelacji post factum. Współczesne rozwiązania zazwyczaj oferują gotowe konektory i adaptery, które upraszczają ten proces. Przykładowo, platforma Feedzai umożliwia wpięcie modułu biometrii behawioralnej zarówno w proces monitorowania transakcji, jak i bezpośrednio do SIEM, niezależnie od tego, czy rozwiązanie działa jako część większego pakietu, czy w wariancie stand-alone, komunikując się z zewnętrznymi systemami poprzez standardowe API i strumienie zdarzeń. Podobną elastyczność deklarują inni dostawcy – BioCatch udostępnia API i mechanizmy regułowe pozwalające zespołom antyfraudowym budować własne korelacje na bazie sygnałów behawioralnych, natomiast Plurilock wskazuje na możliwość redukcji liczby fałszywych alarmów dzięki wzbogacaniu logów SIEM o kontekst behawioralny. W praktyce celem integracji jest zapewnienie, aby każde istotne zdarzenie bezpieczeństwa było opatrzone informacją o tym, czy dana operacja została wykonana w sposób zgodny z typowym profilem użytkownika.

Po włączeniu danych behawioralnych do platform SIEM lub UEBA kluczowe znaczenie ma opracowanie reguł korelacji oraz modeli oceny ryzyka, które pozwolą przełożyć informacje o anomaliach na decyzje operacyjne. Przykładowo, możliwe jest zdefiniowanie reguły zakładającej wygenerowanie alertu typu ATO w sytuacji, gdy w krótkim czasie wystąpi zarówno wysoki wynik ryzyka behawioralnego, jak i nietypowa geolokalizacja logowania. Innym scenariuszem jest korelacja międzykanałowa, w której oznaki stresu lub niepewności użytkownika podczas sesji online, połączone z wykonaniem przelewu powyżej określonego progu na nowego odbiorcę, skutkują alertem potencjalnego oszustwa socjotechnicznego. Takie wielowarstwowe reguły umożliwiają identyfikację złożonych scenariuszy nadużyć, które przy analizie pojedynczych sygnałów mogłyby pozostać niezauważone.

Nowoczesne systemy SIEM, takie jak Splunk Enterprise Security, IBM QRadar czy Elastic Security, wykorzystują mechanizmy scoringu ryzyka, które pozwalają sumować punktację z różnych źródeł dla danego użytkownika, sesji lub urządzenia. W takim modelu pojedyncza anomalia behawioralna nie musi od razu generować alarmu, lecz podnosi ogólny poziom ryzyka, a dopiero przekroczenie ustalonego progu prowadzi do eskalacji incydentu. Pozwala to znacząco ograniczyć liczbę alertów i skupić uwagę zespołów bezpieczeństwa na realnych zagrożeniach. Jednocześnie algorytmy UEBA oparte na AI i uczeniu maszynowym mogą analizować zachowanie użytkowników w dłuższym horyzoncie czasowym, wykrywając powolne, trudne do zauważenia naruszenia, charakterystyczne dla tzw. ataków typu *„slow-and-low”*. Włączenie danych z biometrii behawioralnej zwiększa precyzję takich analiz, umożliwiając wychwycenie nawet niewielkich, lecz systematycznych odchyleń od normalnego wzorca zachowania.

Integracja biometrii behawioralnej z systemami monitoringu bezpieczeństwa wpływa również na sposób pracy zespołów odpowiedzialnych za reagowanie na incydenty, w szczególności Security Operations Center (SOC). Analitycy bezpieczeństwa muszą być przygotowani do interpretowania alertów behawioralnych i zestawiania ich z innymi informacjami dotyczącymi potencjalnego incydentu. Przykładowo sygnał wskazujący na istotne odchylenie od typowej dynamiki interakcji użytkownika może sugerować próbę przejęcia konta. W takiej sytuacji analiza powinna uwzględniać dodatkowe dane kontekstowe, takie jak zmiana adresu IP, charakterystyka urządzenia czy próby realizacji nietypowych operacji. Wielowymiarowe podejście pozwala ograniczyć niepotrzebne eskalacje i kontakt z klientem wyłącznie do przypadków, w których występuje spójny zestaw przesłanek wskazujących na podwyższone ryzyko. Dane behawioralne mogą również przyczyniać się do redukcji liczby fałszywych alarmów. Zdarzenie, które w modelu opartym wyłącznie na parametrach technicznych mogłoby zostać uznane za podejrzane (np. logowanie z nowego urządzenia), może zostać ocenione jako niskiego ryzyka, jeśli wzorzec interakcji pozostaje zgodny z profilem użytkownika. Pozwala to zespołom SOC koncentrować się na incydentach rzeczywiście wymagających reakcji.

Ciągły monitoring behawioralny sprzyja także szybszemu reagowaniu na ataki w toku. W przypadku przejęcia sesji użytkownika każda nietypowa sekwencja działań, taka jak nagłe dodanie nowego odbiorcy i próba wykonania przelewu, może wygenerować natychmiastowy alert, umożliwiający reakcję jeszcze w trakcie trwania ataku, np. poprzez przerwanie sesji za pomocą mechanizmów SOAR. Badania wskazują, że wzbogacenie danych SIEM o sygnały behawioralne skraca średni czas wykrycia i reakcji na incydent (MTTD/MTTR), dzięki lepszemu kontekstowi zdarzeń.

Doświadczenia rynkowe pokazują, że integracja biometrii behawioralnej z istniejącą infrastrukturą bez-

pieczeństwa przynosi wymierne korzyści. W Stanach Zjednoczonych duże instytucje finansowe wykorzystują dane behawioralne w systemach wykrywania zagrożeń wewnętrznych, aby identyfikować pracowników mogących nadużywać dostępu do systemów. W Europie[173] coraz częściej spotyka się modele ścisłej współpracy między zespołami antifraud a SOC[174], w których jedno zdarzenie wykryte w kanale transakcyjnym generuje jednocześnie sprawę operacyjną i incydent bezpieczeństwa. W Polsce zaawansowanym przykładem jest sektorowa platforma BIK, gdzie podejrzane profile zachowań wykryte w jednym banku mogą zasilać systemy pozostałych instytucji, umożliwiając szybką reakcję na próby wykorzystania tych samych danych w innym banku. Takie podejście pozwala ograniczyć problem tzw. *cold start* i pokazuje, że integracja sygnałów behawioralnych zachodzi nie tylko wewnątrz organizacji, lecz także na poziomie całego sektora.

Podsumowując, integracja biometrii behawioralnej z systemami monitoringu zdarzeń bezpieczeństwa oraz mechanizmami reagowania na incydenty wzmacnia zdolność banku do wczesnego wykrywania anomalii i korelowania rozproszonych sygnałów ryzyka. Umożliwia to realizację modelu ciągłej, kontekstowej oceny aktywności użytkownika, zgodnego z podejściem Zero Trust, w którym zaufanie podlega stałej weryfikacji. Centralizacja analizy zdarzeń w ramach zespołów odpowiedzialnych za bezpieczeństwo pozwala szybciej łączyć pozornie niezależne incydenty – zarówno w obszarze relacji z klientami, jak i w przypadku zagrożeń wewnętrznych związanych z dostępem do systemów bankowych. W efekcie instytucja może skrócić czas wykrycia nieprawidłowości, ograniczyć liczbę fałszywych alarmów oraz utrzymać wysoki poziom ochrony przy minimalnym wpływie na doświadczenie użytkowników.

5.3. Wsparcie procesów zgodności (compliance) – AML, PSD2, DORA, NIS2

Biometria behawioralna bywa wdrażana w bankach przede wszystkim jako mechanizm ograniczania oszustw, jednak w praktyce jej rola wykracza poza *„fraud detection”* i obejmuje wsparcie procesów zgodności. Wynika to z faktu, że rozwiązania behawioralne dostarczają dodatkowej warstwy ciągłego monitorowania aktywności, opartej na analizie anomalii w sposobie działania użytkownika, co może zasilać zarówno mechanizmy bezpieczeństwa, jak i funkcje kontrolne oraz dowodowe (*audit trail*) w ramach compliance[175].

5.3.1. DORA i zgodność w obszarze ICT oraz NIS2

W modelu zrekonstruowanym z DORA kluczowe jest, aby podmiot finansowy był zdolny do wczesnego i skutecznego wykrywania nietypowych działań poprzez gromadzenie, monitorowanie i analizę różnych źródeł informacji, a nie wyłącznie logów systemowych, oraz by właściwie przypisać role i obowiązki w tym zakresie. Jednocześnie – w zakresie, w jakim takie informacje mogą obejmować dane osobowe – wymagane jest ograniczenie ich do tego, co niezbędne dla celów wykrywania incydentów[176]. W praktyce biometria behawioralna może pełnić rolę źródła sygnału ryzyka (*risk signal*), który wspiera procesy decyzyjne (np. podniesienie poziomu uwierzytelnienia, wstrzymanie operacji, wszczęcie sprawy kontrolnej), a jednocześnie pomaga budować dowody dotyczące incydentów oraz uzasadnienie reakcji operacyj-

173 UK Finance (2025) – „Annual Fraud Report 2025”. Raport branżowy UK Finance o oszustwach płatniczych.

174 Infosys (2022) – „Adopt Behavioral Biometrics and Analytics for Effective Cybersecurity and Fraud Management.

175 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 (DORA) oraz rozporządzenie delegowane Komisji (UE) 2024/1774, które akcentują konieczność ciągłego monitorowania, wykrywania nietypowych działań oraz analizy wielu źródeł informacji w celu wczesnej identyfikacji incydentów związanych z ICT, przy jednoczesnym zapewnieniu proporcjonalności i minimalizacji przetwarzanych danych osobowych. W tym ujęciu rozwiązania analizy behawioralnej mogą stanowić uzupełniające źródło sygnałów ryzyka oraz materiał dowodowy wspierający procesy kontrolne i zarządzanie incydentami. Zob. także ISO/IEC 27001:2022, w szczególności wymagania dotyczące monitorowania, pomiarów, analizy i oceny skuteczności zabezpieczeń oraz utrzymywania udokumentowanych informacji jako dowodów funkcjonowania systemu zarządzania bezpieczeństwem informacji.

176 W związku z rozporządzeniem delegowanym Komisji (UE) 2024/1774 uzupełniającym DORA, w szczególności motywy oraz przepisy dotyczące ustanawiania polityk i procedur bezpieczeństwa ICT, które wymagają od podmiotów finansowych gromadzenia, monitorowania i analizowania informacji pochodzących z różnych źródeł w celu wczesnego wykrywania nietypowych działań i incydentów związanych z ICT, przy jednoczesnym jasnym przypisaniu ról i obowiązków w tym zakresie. Akt ten podkreśla również, że w zakresie, w jakim przetwarzane informacje stanowią dane osobowe, powinny one być ograniczone do tego, co jest niezbędne dla celów wykrywania incydentów, zgodnie z zasadą minimalizacji danych.

nej[177]. Z perspektywy spójności compliance istotne jest, że NIS2 dopuszcza pierwszeństwo sektorowych aktów UE w zakresie środków zarządzania ryzykiem w cyberbezpieczeństwie i zgłaszania incydentów, o ile są one co najmniej równoważne, a także akcentuje potrzebę zapewnienia spójności oraz dostępu CSIRT/właściwych organów do zgłoszeń incydentów w modelu sektorowym[178]. Równolegle uzasadnienie DORA wskazuje, że w obszarze usług finansowych DORA podnosi poziom harmonizacji i rygoru wymogów w zakresie zarządzania ryzykiem ICT i zgłaszania incydentów, stanowiąc w tym zakresie lex specialis względem NIS2[179]. W konsekwencji biometria behawioralna – jako mechanizm detekcyjny i kontekstowy – może wspierać bank w realizacji obowiązków compliance zarówno w logice DORA (operacyjna odporność cyfrowa), jak i w szerszym porządku NIS2 (zarządzanie ryzykiem i incydentami), bez tworzenia „równoległych reżimów" kontrolnych.

5.3.2. ISO/IEC 27001 jako element systemowego zarządzania ryzykiem i podstawa dowodowa

ISO/IEC 27001 nie jest aktem regulacyjnym sensu stricto, lecz normą ustanawiającą system zarządzania bezpieczeństwem informacji (ISMS), którego centralnym elementem jest podejście oparte na analizie i traktowaniu ryzyka. Włączenie biometrii behawioralnej do architektury bezpieczeństwa może stanowić element realizacji obowiązku identyfikacji, oceny i monitorowania ryzyk związanych z bezpieczeństwem informacji[180]. Norma wymaga m.in. określenia sposobu monitorowania skuteczności zabezpieczeń (clause 9.1), prowadzenia udokumentowanych informacji (clause 7.5) oraz uwzględniania wymagań regulacyjnych stron zainteresowanych w kontekście organizacji (clause 4.2). Oznacza to, że mechanizmy detekcyjne – w tym systemy analizy behawioralnej – powinny być nie tylko wdrożone technicznie, lecz także objęte formalnym nadzorem, pomiarem skuteczności i dokumentowaniem wyników[181].

Z perspektywy praktycznej biometria behawioralna może wspierać[182]:

(i) proces identyfikacji i aktualizacji ryzyk w ramach ISMS,

(ii) bieżące monitorowanie skuteczności zabezpieczeń,

(iii) gromadzenie materiału dowodowego wykorzystywanego w audytach wewnętrznych i zewnętrznych.

177 W tym zakresie szczególnie rozporządzenie delegowane Komisji (UE) 2024/1774 uzupełniające DORA, które zakłada wykorzystanie wyników monitorowania i analizy nietypowych działań jako podstawy do podejmowania adekwatnych środków zarządzania ryzykiem związanym z ICT, w tym eskalacji, ograniczenia lub wstrzymania operacji oraz uruchamiania procedur reagowania na incydenty. W tym kontekście sygnały ryzyka mogą stanowić element materiału dowodowego dokumentującego przebieg incydentu i zasadność podjętych działań. Zob. także ISO/IEC 27001:2022, w szczególności wymagania dotyczące monitorowania, analizy i oceny (cl. 9.1) oraz utrzymywania udokumentowanych informacji jako dowodów funkcjonowania i skuteczności systemu zarządzania bezpieczeństwem informacji.

178 W tym wypadku NIS2, jako dyrektywa, która dopuszcza stosowanie sektorowych aktów Unii Europejskiej w zakresie środków zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązków zgłaszania incydentów, pod warunkiem że zapewniają one poziom ochrony co najmniej równoważny wymaganiom NIS2. Dyrektywa ta akcentuje jednocześnie konieczność zapewnienia spójności systemowej oraz skutecznego dostępu właściwych organów i zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) do informacji o incydentach, w tym w modelach sektorowych.

179 Szczególnie motywy DORA, , które wskazują, że celem tego aktu jest ustanowienie jednolitych, sektorowych wymogów w zakresie zarządzania ryzykiem związanym z ICT oraz zgłaszania incydentów dla podmiotów finansowych, w celu zapewnienia wysokiego poziomu harmonizacji i operacyjnej odporności cyfrowej w całym sektorze finansowym Unii. Uzasadnienie DORA podkreśla, że regulacja ta ma charakter szczególny wobec horyzontalnych ram cyberbezpieczeństwa, w tym dyrektywy (UE) 2022/2555 (NIS2), i ma zapobiegać rozdrobnieniu regulacyjnemu poprzez zastosowanie spójnego reżimu sektorowego.

180 W związku z ISO/IEC 27001:2022, w szczególności wymagania dotyczące monitorowania, pomiarów, analizy i oceny (pkt 9.1), które zobowiązują organizację do określenia, co podlega monitorowaniu i pomiarom, jakimi metodami oraz w jaki sposób oceniana jest skuteczność zabezpieczeń i procesów bezpieczeństwa informacji. Norma wymaga również utrzymywania udokumentowanych informacji jako dowodów wyników monitorowania i oceny funkcjonowania systemu zarządzania bezpieczeństwem informacji, co ma kluczowe znaczenie z perspektywy audytowalności i compliance.

181 Tamże.

182 W tym wypadku również ISO/IEC 27001:2022, ale w szczególności wymagania dotyczące szacowania i postępowania z ryzykiem w bezpieczeństwie informacji (pkt 6.1), monitorowania, pomiarów, analizy i oceny (pkt 9.1) oraz utrzymywania udokumentowanych informacji jako dowodów funkcjonowania systemu zarządzania bezpieczeństwem informacji (pkt 7.5). W tym ujęciu sygnały anomalii mogą stanowić wejście do procesu oceny ryzyka, zasilać monitoring i raportowanie w ramach ISMS oraz wspierać zapewnienie śladowości (traceability) decyzji i reakcji operacyjnych na potrzeby audytu i compliance.

W tym ujęciu compliance nie jest odrębnym procesem, lecz rezultatem prawidłowo funkcjonującego systemu zarządzania ryzykiem bezpieczeństwa informacji.

5.3.3. AML i PSD2

W obszarach AML i PSD2 (w szczególności tam, gdzie zgodność wymaga silnej kontroli ryzyka nadużyć i wiarygodności kanałów cyfrowych) biometria behawioralna może pełnić rolę dodatkowego mechanizmu wykrywania anomalii i ograniczania nadużyć, zwłaszcza w sytuacjach, gdy użytkownik działa z prawidłowymi poświadczeniami, ale sposób działania wskazuje na przejęcie sesji, automatyzację lub manipulację. W ujęciu compliance jest to istotne, ponieważ cyberincydenty w sektorze finansowym przekładają się nie tylko na straty i zakłócenia operacyjne, ale również na ryzyko niezgodności regulacyjnej i utratę zaufania[183].

5.3.4. Wnioski cząstkowe

W ocenie autorów, w takiej sytuacji, biometria behawioralna może być traktowana jako komponent, który łączy funkcje bezpieczeństwa, zarządzania ryzykiem i compliance, ponieważ dostarcza mierzalnego sygnału o anomaliach zachowania, ułatwia korelację w ekosystemie detekcji oraz wzmacnia dowodowość działań banku. Jej największa wartość ujawnia się wtedy, gdy jest osadzona w ramach zarządzania ryzykiem ICT oraz praktyk monitorowania i dokumentowania, zgodnych z DORA/NIS2 i wymaganiami systemowymi ISO/IEC 27001.

5.4. Efektywność w kontekście nowych zagrożeń (deepfake, przejęcia kont, ataki socjotechniczne)

Współczesny paradygmat cyberbezpieczeństwa w sektorze bankowym przechodzi fundamentalną metamorfozę, wymuszoną przez dynamiczną ewolucję wektorów ataku oraz rosnące wyrafinowanie grup przestępczych. Tradycyjne modele ochrony, oparte na statycznej weryfikacji tożsamości w momencie logowania odchodzą do przeszłości. Statyczne zabezpieczenia, takie jak hasła czy jednorazowe kody SMS (OTP), okazały się niewystarczające w obliczu zagrożeń wykorzystujących inżynierię społeczną, automatyzację oraz syntetyczne media generowane przez sztuczną inteligencję.

W odpowiedzi na te wyzwania, instytucje finansowe coraz powszechniej adaptują rozwiązania z zakresu biometrii behawioralnej – technologii analizującej unikalne wzorce interakcji użytkownika z urządzeniem, obejmujące dynamikę pisania, ruchy kursora, gesty na ekranach dotykowych oraz sposób trzymania urządzenia (analiza danych z żyroskopu i akcelerometru).

Efektywność systemów bezpieczeństwa nie powinna być już definiowana binarnie (dostęp przyznany/odmowa), lecz jako funkcja zdolności systemu do ciągłej oceny ryzyka w czasie rzeczywistym. Biometria behawioralna, działając w trybie pasywnym i transparentnym dla użytkownika, umożliwia wykrywanie anomalii niewidocznych dla tradycyjnych systemów antyfraudowych, które opierają się na analizie urządzenia (*device fingerprinting*) czy geolokalizacji.

5.4.1. Deepfake

Rozwój generatywnej sztucznej inteligencji (GenAI) wprowadził do arsenału cyberprzestępców narzędzia o bezprecedensowej sile rażenia. Technologia deepfake umożliwia tworzenie hiperrealistycznych

183 W związku z DORA oraz rozporządzeniem delegowanym Komisji (UE) 2024/1774, które akcentują konieczność wykrywania nietypowych działań i incydentów związanych z ICT, w tym sytuacji, w których działania wykonywane są z użyciem prawidłowych poświadczeń, lecz w sposób odbiegający od normalnego wzorca, oraz podejmowania adekwatnych środków ograniczających ryzyko. Zob. także dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), która wiąże zarządzanie ryzykiem w cyberbezpieczeństwie z ograniczaniem skutków incydentów dla ciągłości działania, zgodności regulacyjnej i zaufania do usług cyfrowych. W tym kontekście mechanizmy detekcji anomalii mogą wspierać realizację obowiązków compliance w obszarach wymagających szczególnej kontroli ryzyka nadużyć w kanałach cyfrowych.

klonów głosowych oraz wideo, które mogą być wykorzystywane do omijania weryfikacji tożsamości.

Najnowsze raporty branżowe potwierdzają dalszą eskalację zagrożeń związanych z deepfake'ami w procesach zdalnej weryfikacji tożsamości – według danych raportu opracowanego przez Sumsub[184] liczba wykrywanych ataków tego typu wzrosła kilkukrotnie w latach 2023–2024, natomiast raport iProov[185] wskazuje na bezprecedensowy wzrost zaawansowanych ataków typu *face swap* oraz *digital injection* w 2024 r., co potwierdza trwałe umocnienie się deepfake'ów jako jednego z kluczowych wektorów nadużyć w systemach identyfikacji cyfrowej.

W walce z zagrożeniami syntetycznymi biometria behawioralna pełni rolę kluczowego mechanizmu weryfikacji żywotności (ang. *Liveness Detection*):

- **Pasywna detekcja żywotności.** Zgodnie z normą ISO/IEC 30107–3:2023[186], systemy biometryczne muszą być odporne na ataki prezentacyjne (PAD). Rozwiązania behawioralne analizują mikroruchy głowy i gałek ocznych oraz zmiany w teksturze skóry, które nie występują w maskach czy projekcjach wideo. W podejściu pasywnym nacisk kładzie się nie na wykonywanie przez użytkownika zadań *„challenge-response"*, lecz na statystyczną ocenę zgodności obserwowanej dynamiki z rozkładami typowymi dla prezentacji *bona fide*.
- **Obrona przed atakami iniekcyjnymi.** Biometria behawioralna wykrywa brak spójności multimodalnej. Jeśli system otrzymuje idealnie stabilny obraz wideo, ale akcelerometr urządzenia nie rejestruje mikrodrżeń ręki typowych dla trzymania telefonu, jest to sygnał, że obraz nie pochodzi z fizycznego sensora (atak typu *video injection*)[187].
- **Analiza artefaktów generatywnych.** Algorytmy wykorzystywane w systemach biometrycznych mogą uwzględniać charakterystyczne artefakty pozostawiane przez modele generatywne stosowane w tworzeniu deepfake'ów audio i wideo. Jednym z kluczowych obszarów jest analiza synchronizacji pomiędzy ruchem ust a sygnałem fonetycznym, gdzie nawet zaawansowane modele syntezy mowy i obrazu wykazują drobne, lecz statystycznie istotne opóźnienia, nieliniowości lub niespójności w przejściach artykulacyjnych. Odchylenia te są trudne do zauważenia dla człowieka, lecz możliwe do wykrycia przez modele uczone na rzeczywistych nagraniach interakcji człowiek-maszyna. Wartym uwagi są anomalie w mikrozachowaniach fizjologicznych, takich jak częstotliwość, regularność i amplituda mrugania. W naturalnych warunkach mruganie jest procesem nieregularnym, zależnym od zmęczenia, stresu i bodźców wzrokowych, natomiast w materiałach syntetycznych często występują wzorce regularne, zbyt rzadkie albo nienaturalnie zsynchronizowane z innymi ruchami twarzy. Podobne artefakty dotyczą mikroekspresji, minimalnych ruchów mięśni twarzy oraz przejść między pozycjami głowy, które w treściach generowanych bywają nadmiernie wygładzone lub pozbawione losowej zmienności. Z perspektywy biometrii behawioralnej kluczowe znaczenie ma to, że analiza takich artefaktów opiera się na **korelacji w czasie** oraz na zgodności z kontekstem sesji. Niespójność pomiędzy ruchem ust, sygnałem głosowym i danymi kontekstowymi (np. czas reakcji użytkownika) może wskazywać na wykorzystanie treści generatywnych, nawet jeśli pojedynczy kanał wygląda na wiarygodny[188].

5.4.2. Przejmowanie kont

Zjawisko przejmowania kont (ATO) stanowi jedno z najpoważniejszych wyzwań dla współczesnej bankowości. Organizacje przestępcze wykorzystują zautomatyzowane narzędzia do *credential stuffing* (masowego testowania par login-hasło) oraz zaawansowane złośliwe oprogramowanie (malware), w tym trojany zdalnego dostępu (RAT). W kontekście ATO, biometria behawioralna koncentruje się na rozróżnieniu między prawowitym użytkownikiem a intruzem. Kluczową przewagą tej technologii jest analiza profilu kognitywno-motorycznego, który jest niezwykle trudny do sfałszowania.

184 https://sumsub.com/blog/fraud-trends-sumsub-fraud-report.

185 https://www.iproov.com/reports/threat-intelligence-report-2025-remote-identity-attack.

186 https://www.iso.org/standard/79520.html.

187 Veriff. (2024). Identity Fraud Report 2024. Veriff Industry Insights. https://www.veriff.com/resources/ebooks/fraud-report-2024.

188 Nguyen, T. T., et al. (2022). Deep learning for deepfakes creation and detection: A survey. Computer Vision and Image Understanding, 223, 103525

Wybrane ataki:

- **Atak zautomatyzowany.** Nadludzka szybkość wprowadzania danych, idealnie równe odstępy czasowe między zdarzeniami, liniowe ruchy myszą, brak wahań decyzyjnych. |Analiza mikroruchów i entropii zachowania. Boty wykazują niską entropię i wysoką powtarzalność. Systemy behawioralne wykrywają brak naturalnych fluktuacji ludzkich.
- **Zdalny dostęp.** Mysz porusza się w sposób "skokowy" lub z nienaturalnym opóźnieniem sieciowym. Brak mikroruchów dłoni na urządzeniu mobilnym skorelowanych z aktywnością na ekranie. |Wykrywanie anomalii w protokole zdalnym oraz brak korelacji między sensorami (np. dotyk ekranu bez zmiany odczytu akcelerometru).
- **Ludzki intruz.** Używanie skrótów klawiszowych (Ctrl+C/CTRL+V) do danych, które właściciel zna na pamięć (adres, nazwisko). Nawigacja celowa, „tunelowa", szybkie przejście do transferu środków.
- **Symulatory Urządzeń (Emulatory).** Generowanie zdarzeń dotykowych niemożliwych anatomicznie (np. idealny środek przycisku, brak zmiany kąta nachylenia telefonu). Analiza powierzchni dotyku i danych żyroskopowych. Weryfikacja fizycznej obecności urządzenia w ręku użytkownika.

5.4.3. Ataki socjotechniczne

Współczesna cyberprzestępczość ewoluuje w kierunku ataków, które omijają zabezpieczenia techniczne, celując bezpośrednio w najsłabsze ogniwo systemu – człowieka. Oszustwa typu *Authorized Push Payment (APP)*, w których zmanipulowana ofiara sama autoryzuje transakcję, stanowią rosnący odsetek strat. W takich scenariuszach tradycyjne metody uwierzytelniania zawodzą, ponieważ to uprawniony użytkownik loguje się z zaufanego urządzenia.

Biometria behawioralna oferuje unikalną możliwość detekcji ataków socjotechnicznych poprzez analizę stanu emocjonalnego i kognitywnego użytkownika. Systemy te poszukują tzw. „cyfrowych tików" – subtelnych anomalii w zachowaniu, które wskazują, że użytkownik działa pod wpływem stresu lub instrukcji osoby trzeciej.

Rozdział 6. Aspekty prawne i etyczne

6.1. Biometria behawioralna a ochrona danych osobowych (RODO, eIDAS 2, AI Act)

Biometria behawioralna wpisuje się w normatywny model tożsamości cyfrowej jako szczególny rodzaj atrybutu, który nie opisuje osoby w sposób statyczny, lecz ujawnia się poprzez jej zachowanie w określonym kontekście użycia systemu informatycznego. W przeciwieństwie do klasycznych danych identyfikacyjnych, takich jak imię i nazwisko czy numer identyfikacyjny, a także w odróżnieniu od biometrii fizycznej, biometria behawioralna nie stanowi trwałego „znacznika" osoby, lecz dynamiczny wzorzec aktywności, który jest rekonstruowany i oceniany na podstawie obserwacji sposobu interakcji użytkownika z systemem[189].

Tak rozumiana biometria behawioralna pozostaje spójna z koncepcją tożsamości cyfrowej jako konstrukcji relacyjnej i kontekstowej, przyjętą w prawie Unii Europejskiej. Jak wykazano w poprzednich rozdziałach, tożsamość cyfrowa nie funkcjonuje jako autonomiczny byt, lecz jako zbiór atrybutów wykorzystywanych selektywnie w relacjach pomiędzy użytkownikiem a stronami ufającymi, w zależności od celu danej interakcji oraz poziomu ryzyka z nią związanego[190]. Biometria behawioralna może w tym ujęciu pełnić funkcję atrybutu wspierającego proces uwierzytelniania, którego znaczenie ujawnia się wyłącznie w określonym kontekście operacyjnym, takim jak dostęp do usługi, autoryzacja czynności lub ciągła ocena integralności sesji użytkownika[191].

Specyfika biometrii behawioralnej polega na tym, że atrybut ten nie jest przekazywany w sposób jednorazowy ani wyraźnie zadeklarowany przez użytkownika, lecz powstaje w toku bieżącej analizy jego zachowania. W praktyce oznacza to, że granica pomiędzy danymi wykorzystywanymi do uwierzytelniania a danymi generowanymi jako produkt uboczny korzystania z systemu ulega zatarciu. Z perspektywy konstrukcji tożsamości cyfrowej biometria behawioralna stanowi zatem atrybut o podwyższonej wrażliwości normatywnej, ponieważ jej pozyskiwanie i przetwarzanie może następować w sposób ciągły, często bez wyraźnego momentu inicjalnego, który byłby jednoznacznie identyfikowalny dla użytkownika[192].

Jednocześnie biometria behawioralna różni się zasadniczo od tradycyjnych atrybutów tożsamości cyfrowej tym, że jej wartość identyfikacyjna ma charakter probabilistyczny. Nie polega ona na prostym potwierdzeniu określonej cechy osoby, lecz na statystycznym dopasowaniu obserwowanego wzorca zachowania do profilu przypisanego danemu użytkownikowi. W konsekwencji biometria behawioralna nie funkcjonuje jako samodzielny nośnik tożsamości, lecz jako element wspierający ocenę wiarygodności relacji pomiędzy podmiotem a wykorzystywanymi atrybutami. Taki charakter wpisuje się w rozwijany w prawie Unii Europejskiej model uwierzytelniania kontekstowego, w którym tożsamość nie jest ustalana w sposób absolutny, lecz oceniana w zależności od okoliczności konkretnej interakcji[193].

Z perspektywy prawnej istotne znaczenie ma również fakt, że biometria behawioralna, jako atrybut tożsamości cyfrowej, może być wykorzystywana zarówno w modelach scentralizowanych, jak i w bardziej złożonych architekturach relacyjnych, w tym w ramach ekosystemów opartych na zaufaniu regulacyjnym. Niezależnie jednak od przyjętego modelu zarządzania tożsamością, jej wykorzystanie prowadzi do przetwarzania informacji, które pozostają ściśle powiązane z osobą fizyczną i jej sposobem funkcjonowania w środowisku cyfrowym. Oznacza to, że biometria behawioralna nie może być traktowana wyłącznie jako neutralny parametr techniczny, lecz powinna być

189 Zob. rozdział 2., szerzej: rozważania dotyczące atrybutów tożsamości cyfrowej, ich kontekstowego i relacyjnego charakteru oraz odejścia od statycznego modelu identyfikacji w środowisku cyfrowym.

190 Por. analizę pojęcia tożsamości cyfrowej jako konstrukcji relacyjnej i kontekstowej, opartej na selektywnym wykorzystywaniu atrybutów w relacjach pomiędzy użytkownikiem a stronami ufającymi, przedstawioną w rozdziale 2. niniejszego raportu.

191 Zob. rozważania dotyczące mechanizmów uwierzytelniania jako funkcjonalnego elementu tożsamości cyfrowej oraz ich kontekstowego charakteru, zależnego od celu interakcji i poziomu ryzyka, przedstawione w rozdziale 2. w podrozdziałach 1. i 3. niniejszego opracowania.

192 Tamże.

193 Zob. normatywne ujęcie uwierzytelniania jako procesu oceny wiarygodności, a nie absolutnego ustalenia tożsamości, w relacyjnym modelu tożsamości cyfrowej przyjętym w prawie Unii Europejskiej w rozdziale 2.

analizowana jako element konstrukcji tożsamości cyfrowej, podlegający ocenie z perspektywy ochrony danych osobowych oraz praw podstawowych[194].

Takie ujęcie biometrii behawioralnej jako atrybutu tożsamości cyfrowej stanowi punkt wyjścia do dalszych rozważań dotyczących jej kwalifikacji prawnej, proporcjonalności stosowania oraz wpływu na transparentność i zaufanie użytkowników. W kolejnych podrozdziałach zostanie wykazane, że dynamiczny, ciągły i często niejawny charakter tego atrybutu uzasadnia szczególnie rygorystyczne podejście regulacyjne, zarówno na gruncie RODO, jak i w świetle eIDAS 2 oraz AI Act[195].

6.2. Proporcjonalność i minimalizacja danych

Zastosowanie biometrii behawioralnej w systemach tożsamości cyfrowej wymaga nie tylko formalnej zgodności z przesłankami legalności przetwarzania danych osobowych, lecz także spełnienia podstawowych zasad przetwarzania określonych w RODO, w szczególności zasady proporcjonalności oraz minimalizacji danych. W przeciwieństwie do klasycznych metod uwierzytelniania, biometria behawioralna charakteryzuje się bowiem zdolnością do ciągłego i kontekstowego pozyskiwania informacji o użytkowniku, co znacząco zwiększa ryzyko nadmiernej ingerencji w sferę prywatności. Ocena dopuszczalności takich rozwiązań nie może zatem ograniczać się do pytania o to, czy dane przetwarzanie jest możliwe, lecz powinna obejmować analizę, czy zakres, intensywność oraz czas trwania przetwarzania pozostają niezbędne i adekwatne do realizowanego celu. W tym ujęciu zasada proporcjonalności staje się kluczowym kryterium wyznaczającym granice dopuszczalnego wykorzystania biometrii behawioralnej, determinując zarówno projektowanie systemów, jak i sposób ich praktycznego stosowania[196].

Zasada minimalizacji danych, wyrażona w art. 5 ust. 1 lit. c RODO, nabiera szczególnego znaczenia w przypadku systemów opartych na biometrii behawioralnej, ponieważ ich funkcjonowanie z natury rzeczy opiera się na gromadzeniu i analizie dużej liczby sygnałów dotyczących zachowania użytkownika. W tym kontekście minimalizacja nie może być rozumiana wyłącznie jako ograniczenie zakresu zbieranych danych na etapie inicjalnym, lecz obejmuje również sposób ich dalszego przetwarzania, częstotliwość aktualizacji profili behawioralnych oraz okres przechowywania uzyskanych wzorców. W praktyce oznacza to konieczność krytycznej oceny, czy wszystkie wykorzystywane cechy behawioralne są rzeczywiście niezbędne do osiągnięcia zakładanego celu uwierzytelnienia, czy też pełnią jedynie funkcję pomocniczą lub historyczną, zwiększając ryzyko nadmiernej ingerencji w prywatność. Minimalizacja danych w systemach biometrii behawioralnej powinna zatem obejmować zarówno selekcję atrybutów, jak i ograniczenie intensywności oraz czasu trwania przetwarzania, co bezpośrednio wpływa na ocenę proporcjonalności całego rozwiązania[197].

W praktyce stosowania biometrii behawioralnej kluczowym instrumentem służącym weryfikacji spełnienia zasady proporcjonalności oraz minimalizacji danych staje się ocena skutków dla ochrony danych (DPIA), o której mowa w art. 35 RODO. Ze względu na systematyczne monitorowanie zachowania użytkownika, wykorzystanie nowych technologii oraz potencjalnie znaczący wpływ na prawa i wolności osób fizycznych, przetwarzanie biometrii behawioralnej co do zasady mieści się w katalogu operacji wymagających przeprowadzenia takiej oceny. DPIA powinna w tym kontekście obejmować nie tylko identyfikację ryzyk związanych z nieuprawnioną identyfikacją lub wtórnym wykorzystaniem danych behawioralnych, lecz także analizę konieczności i proporcjonalności planowanych operacji przetwarzania w relacji do zamierzonego celu. Oznacza to, że ocena skutków nie może ograniczać się do formalnego opisu systemu, lecz powinna prowadzić do realnej weryfikacji, czy zastosowanie biometrii behawioralnej jest rozwiązaniem niezbędnym, czy też możliwe jest osiągnięcie

194 Zob. w rozdziale 2. normatywne ujęcie tożsamości cyfrowej jako instrumentu prawnie relewantnej reprezentacji osoby fizycznej w środowisku cyfrowym, niezależnie od przyjętego modelu zarządzania tożsamością, oraz wynikającą z tego konieczność oceny wykorzystywanych atrybutów z perspektywy ochrony danych osobowych i praw podstawowych.

195 Zob. w rozdziale 2. analizę modeli zarządzania tożsamością cyfrową, ich relacyjnego charakteru oraz znaczenia tożsamości jako konstrukcji prawno-technicznej, powiązanej z osobą fizyczną i wywołującej skutki prawne w relacjach z różnymi stronami ufającymi, przedstawioną w rozdziałach 1. i 2. niniejszego opracowania.

196 Wynika to z art. 5 ust. 1 lit. RODO, ustanawiający zasadę minimalizacji danych; por. także art. 5 ust. 1 lit. a RODO w zakresie wymogu rzetelności i proporcjonalności przetwarzania danych osobowych.

197 Wynika to z art. 5 ust. 1 lit. c RODO; por. także art. 25 ust. 1 RODO, ustanawiający zasadę ochrony danych w fazie projektowania i domyślnej ochrony danych (*privacy by design i privacy by default*).

porównywalnego poziomu bezpieczeństwa przy użyciu mniej ingerujących środków[198].

Tendencja ta znajduje potwierdzenie w projekcie rozporządzenia COM (2023) 367, który dopuszcza wykorzystanie cech behawioralnych użytkownika w ramach mechanizmów monitorowania transakcji, jednak wyłącznie pod warunkiem spełnienia rygorystycznych wymogów proporcjonalności, minimalizacji danych oraz uprzedniego przeprowadzenia oceny skutków dla ochrony danych[199].

Istotnym elementem testu proporcjonalności w przypadku biometrii behawioralnej jest również obowiązek rozważenia, czy zamierzony cel przetwarzania nie może zostać osiągnięty przy użyciu alternatywnych, mniej ingerujących mechanizmów uwierzytelniania lub kontroli dostępu. W praktyce oznacza to konieczność porównania biometrii behawioralnej z innymi rozwiązaniami technicznymi, takimi jak uwierzytelnianie wieloskładnikowe oparte na wiedzy lub posiadaniu, mechanizmy jednorazowej autoryzacji czy rozwiązania ograniczające się do incydentalnej weryfikacji tożsamości. Jeżeli porównywalny poziom bezpieczeństwa może zostać osiągnięty bez ciągłego monitorowania zachowania użytkownika, zastosowanie biometrii behawioralnej może zostać uznane za nieproporcjonalne, niezależnie od formalnej zgodności z przesłankami legalności przetwarzania. W tym sensie zasada proporcjonalności pełni funkcję materialnej granicy projektowania systemów, wymagając od administratorów nie tylko wykazania skuteczności przyjętego rozwiązania, lecz także jego niezbędności w świetle dostępnych alternatyw[200].

Przeprowadzona analiza pokazuje, że nawet formalnie dopuszczalne wykorzystanie biometrii behawioralnej może naruszać wymagania RODO, jeżeli nie spełnia testu proporcjonalności i minimalizacji danych. W przypadku rozwiązań opartych na ciągłych i niejawnych mechanizmach analizy zachowania szczególnego znaczenia nabiera nie tylko zakres przetwarzanych informacji, lecz także sposób ich komunikowania osobom, których dane dotyczą. W konsekwencji zagadnienie proporcjonalności pozostaje ściśle powiązane z wymogami transparentności oraz akceptacji społecznej, które stanowią przedmiot kolejnego podrozdziału.

6.3. Transparentność i akceptacja społeczna

Wykorzystanie biometrii behawioralnej w systemach tożsamości cyfrowej w sposób szczególny uwidacznia znaczenie zasady transparentności przetwarzania danych osobowych, stanowiącej jeden z fundamentów ochrony praw osób, których dane dotyczą. Ze względu na dynamiczny, ciągły i często niejawny charakter analizy zachowania użytkownika, biometria behawioralna może pozostawać dla osoby fizycznej trudna do zauważenia i zrozumienia, nawet w sytuacjach, w których przetwarzanie to jest formalnie zgodne z przesłankami legalności oraz zasadą proporcjonalności. W tym kontekście transparentność nie ogranicza się do spełnienia minimalnych obowiązków informacyjnych, lecz obejmuje także realną możliwość zrozumienia przez użytkownika, w jaki sposób oraz w jakim celu jego zachowanie jest analizowane. Brak takiej przejrzystości prowadzi nie tylko do osłabienia kontroli osoby nad własnymi danymi, lecz także do erozji zaufania do systemów tożsamości cyfrowej, co w dłuższej perspektywie może podważać społeczną akceptację dla stosowania tego rodzaju rozwiązań[201].

W praktyce realizacja zasady transparentności w odniesieniu do biometrii behawioralnej napotyka jednak istotne ograniczenia wynikające ze złożoności technicznej oraz adaptacyjnego charakteru stosowanych systemów. Informacje przekazywane osobom, których dane dotyczą, nawet jeżeli spełniają formalne wymogi art. 12–14 RODO, często pozostają zbyt abstrakcyjne lub ogólne, aby umożliwić rzeczywiste zrozumienie mechanizmu przetwarzania danych behawioralnych oraz jego konsekwencji. Szczególnym wyzwaniem jest fakt, że wzorce behawioralne nie są przetwarzane w sposób deterministyczny, lecz podlegają ciągłej aktualizacji i ocenie probabili-

198 Wynika to z art. 35 ust. 1–3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), w szczególności w zakresie obowiązku przeprowadzenia oceny skutków w przypadku systematycznego monitorowania oraz wykorzystywania nowych technologii; por. także motyw 84 RODO, podkreślający rolę DPIA jako narzędzia zapobiegania ryzykom dla praw i wolności osób fizycznych.

199 Komisja Europejska, Proposal for a regulation of the european parliament and of the council on payment services in the internal market and amending Regulation (EU) No 1093/2010, Brussels, 28.6.2023 COM(2023) 367 final.

200 Wynika to z art. 5 ust. 1 lit. c RODO w zw. z art. 25 ust. 1 RODO, wymagającymi ograniczenia przetwarzania do zakresu niezbędnego oraz uwzględnienia ochrony danych już na etapie projektowania; zob. także motyw 39 RODO, wskazujący na konieczność przetwarzania danych osobowych tylko w zakresie niezbędnym do realizacji określonych celów.

201 Wynika to z art. 5 ust. 1 lit. a RODO, ustanawiający zasadę rzetelności i przejrzystości przetwarzania danych osobowych, oraz art. 12–14 RODO, określające zakres i sposób realizacji obowiązków informacyjnych wobec osób, których dane dotyczą.

stycznej, co utrudnia jednoznaczne wyjaśnienie, jakie konkretne dane wpływają na wynik procesu uwierzytelniania lub ocenę ryzyka. W konsekwencji może dochodzić do sytuacji, w której transparentność ma charakter jedynie formalny, nie zapewniając użytkownikowi realnej kontroli nad przetwarzaniem jego danych, mimo spełnienia ustawowych obowiązków informacyjnych[202].

Wedle autorów przezwyciężenie opisanych ograniczeń nie polega na dalszym rozszerzaniu zakresu informacji technicznych przekazywanych osobom, których dane dotyczą, lecz na funkcjonalnym przeformułowaniu realizacji zasady transparentności. W przypadku biometrii behawioralnej kluczowe znaczenie ma bowiem nie pełne wyjaśnienie adaptacyjnego i probabilistycznego mechanizmu przetwarzania, lecz zapewnienie użytkownikowi realnej kontroli nad skutkami tego przetwarzania, w szczególności poprzez jasne określenie możliwych konsekwencji, informowanie o interwencjach systemu w toku korzystania z usługi oraz zagwarantowanie możliwości sprzeciwu lub weryfikacji decyzji.

Ograniczona zrozumiałość mechanizmów biometrii behawioralnej wpływa bezpośrednio na zakres autonomii decyzyjnej osoby, której dane dotyczą, a tym samym na realną akceptację społeczną tego rodzaju rozwiązań. Jeżeli użytkownik nie jest w stanie w przystępny sposób zrozumieć, jakie elementy jego zachowania są analizowane, w jakim zakresie oraz z jakimi konsekwencjami, możliwość świadomego podjęcia decyzji dotyczącej korzystania z danej usługi lub wyrażenia zgody na przetwarzanie danych zostanie istotnie ograniczona. W takim ujęciu transparentność przestaje pełnić funkcję gwarancyjną, a staje się jedynie formalnym elementem zgodności regulacyjnej, niewystarczającym do budowania zaufania. Brak rzeczywistej przejrzystości może natomiast prowadzić do społecznego sprzeciwu wobec systemów wykorzystujących biometrię behawioralną, zwłaszcza w sytuacjach, w których ich stosowanie jest postrzegane jako nieproporcjonalne lub trudne do uniknięcia. Tym samym transparentność i akceptacja społeczna pozostają ze sobą ściśle powiązane, a ich niedostateczne zapewnienie zwiększa nie tylko ryzyko naruszenia praw osób fizycznych, lecz także ryzyko prawne i reputacyjne po stronie administratorów danych[203].

Autorzy związku z powyższym wskazują, że transparentność w przypadku biometrii behawioralnej nie ogranicza się do spełnienia obowiązków informacyjnych przewidzianych w art. 12–14 RODO, lecz pełni istotną funkcję w kształtowaniu zaufania użytkowników oraz społecznej akceptacji systemów tożsamości cyfrowej. W praktyce znaczenie to ujawnia się zwłaszcza w odniesieniu do takich mechanizmów jak dynamiczne profilowanie zachowania użytkownika, kontekstowa analiza ryzyka czy adaptacyjne dostosowywanie progów bezpieczeństwa, które, mimo że służą zwiększeniu ochrony przed nadużyciami, mogą prowadzić do trudnych do przewidzenia reakcji systemu, takich jak uruchomienie dodatkowej weryfikacji lub czasowe ograniczenie funkcjonalności usługi.

W sytuacji, gdy sposób działania tych mechanizmów nie jest dla użytkownika dostatecznie zrozumiały, nawet technicznie skuteczne i formalnie zgodne z prawem rozwiązania mogą budzić wątpliwości co do zakresu i zasad przetwarzania danych behawioralnych. Dotyczy to w szczególności przypadków, w których decyzje systemu opierają się na ocenie probabilistycznej lub zmiennym profilu odniesienia, co utrudnia jednoznaczne wskazanie, jakie elementy zachowania miały decydujące znaczenie w danej sytuacji.

W konsekwencji, niewystarczająca transparentność funkcjonowania takich systemów może zwiększać nie tylko ryzyko naruszenia praw osób, których dane dotyczą, lecz także ryzyko prawne i reputacyjne po stronie administratorów danych, zwłaszcza w kontekście oceny proporcjonalności i rozliczalności stosowanych środków bezpieczeństwa. Okoliczności te uzasadniają potrzebę odrębnej analizy transparentności jako czynnika ryzyka w kolejnym podrozdziale.

6.4. Potencjalne ryzyka prawne i reputacyjne

Z perspektywy instytucji finansowych największe ryzyka związane z wykorzystaniem danych behawioralnych nie wynikają z samego faktu zastosowania biometrii, lecz z charakteru przetwarzania danych,

202 Wynika to z art. 12 ust. 1 RODO, wymagający przekazywania informacji w sposób zwięzły, przejrzysty i zrozumiały, oraz motyw 58 RODO, podkreślający konieczność zapewnienia rzeczywistej przejrzystości przetwarzania danych osobowych, a nie jedynie formalnego spełnienia obowiązków informacyjnych.

203 W związku z art. 7 ust. 2 oraz art. 7 ust. 4 RODO, podkreślające znaczenie świadomej i dobrowolnej zgody, a także motyw 42 RODO, wskazujący, że osoba, której dane dotyczą, powinna mieć rzeczywistą możliwość zrozumienia skutków przetwarzania danych osobowych.

jego ciągłości, skali oraz trudności w jednoznacznym określeniu podstawy prawnej. Kluczowe znaczenie ma zatem nie tyle technologia, ile kwalifikacja prawna operacji przetwarzania oraz ich zgodność z wielopoziomowym reżimem regulacyjnym.

W celu uporządkowania analizy zasadne jest rozbicie ryzyk według aktów prawnych, które determinują ramy stosowania analityki behawioralnej w sektorze bankowym.

6.4.1. RODO – podstawa prawna, zgoda i profilowanie

Najbardziej złożone napięcia regulacyjne związane z wykorzystaniem analizy danych behawioralnych w sektorze bankowym ujawniają się na gruncie RODO. Problematyka ta nie dotyczy wyłącznie klasycznej biometrii w rozumieniu technicznym, lecz przede wszystkim kwalifikacji prawnej danych behawioralnych oraz wyboru adekwatnej podstawy przetwarzania w środowisku silnie regulowanym i asymetrycznym, jakim jest relacja bank–klient.

6.4.1.1. Kwalifikacja danych behawioralnych

Dane behawioralne, takie jak dynamika klawiatury (*keystroke dynamics*), wzorce nawigacji w aplikacji mobilnej, tempo reakcji użytkownika, sposób korzystania z interfejsu czy charakterystyka interakcji z urządzeniem, co do zasady stanowią dane osobowe w rozumieniu art. 4 pkt 1 RODO, o ile umożliwiają identyfikację osoby fizycznej bezpośrednio lub pośrednio[204].

W zależności od sposobu ich wykorzystania mogą one jednak przyjmować różny status normatywny. Po pierwsze, mogą być kwalifikowane jako dane wykorzystywane do profilowania w rozumieniu art. 4 pkt 4 RODO, tj. jako dane poddawane zautomatyzowanemu przetwarzaniu w celu oceny niektórych czynników osobowych, w szczególności dotyczących zachowania, preferencji czy wiarygodności użytkownika[205].

Po drugie, w określonych konfiguracjach technologicznych dane behawioralne mogą zostać uznane za dane biometryczne w rozumieniu art. 4 pkt 14 RODO, jeżeli są przetwarzane przy użyciu specjalnych technik w celu jednoznacznej identyfikacji osoby fizycznej[206]. Kluczowe znaczenie ma tu nie rodzaj danych samych w sobie, lecz cel i sposób ich przetwarzania. Oznacza to, że ten sam zestaw sygnałów behawioralnych może w jednym modelu stanowić element analizy ryzyka transakcyjnego, a w innym – mechanizm jednoznacznej identyfikacji użytkownika.

Kwalifikacja ta przesądza o reżimie prawnym przetwarzania oraz o poziomie dopuszczalności operacji analitycznych. W szczególności uznanie danych za biometryczne może prowadzić do zastosowania art. 9 RODO i wymogu spełnienia dodatkowych przesłanek legalizujących przetwarzanie danych szczególnych kategorii[207].

6.4.1.2. Podstawa prawna przetwarzania

W praktyce bankowej najczęściej rozważane są trzy podstawy prawne przetwarzania danych behawioralnych: wykonanie umowy (art. 6 ust. 1 lit. b RODO), prawnie uzasadniony interes administratora (lit. f) oraz zgoda osoby, której dane dotyczą (lit. a).

Odwołanie się do przesłanki wykonania umowy wymaga wykazania, że analiza danych behawioralnych jest obiektywnie niezbędna do realizacji zobowiązania wynikającego z umowy o świadczenie usług bankowych[208]. W wielu przypadkach trudno jednak uznać, że zaawansowana analityka behawioralna jest elementem koniecznym do wykonania podstawowych funkcji rachunku bankowego.

Z kolei konstrukcja prawnie uzasadnionego interesu administratora wymaga przeprowadzenia testu równowagi pomiędzy interesem banku w zakresie zapo-

204 Art. 4 pkt 1 RODO.

205 Art. 4 pkt 4 RODO.

206 Art. 4 pkt 14 RODO.

207 Art. 9 ust. 1–2 RODO.

208 Art. 6 ust. 1 lit. b RODO; zob. także motyw 44 RODO.

biegania nadużyciom, ochrony środków klientów i zapewnienia bezpieczeństwa systemu finansowego, a prawami i wolnościami osób, których dane dotyczą[209]. W kontekście rosnącej liczby ataków typu *account takeover*, fraudów socjotechnicznych czy wykorzystania deepfake'ów argument bezpieczeństwa systemowego zyskuje istotne znaczenie, jednak nie zwalnia administratora z obowiązku wykazania proporcjonalności i minimalizacji przetwarzania.

Najbardziej problematyczną, choć często stosowaną podstawą, pozostaje zgoda osoby, której dane dotyczą. Zgodnie z art. 4 pkt 11 oraz art. 7 RODO zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna[210]. W relacji bank–klient, która ma charakter strukturalnie asymetryczny, pojawia się wątpliwość czy zgoda może być w pełni swobodna, zwłaszcza gdy odmowa jej udzielenia skutkowałaby ograniczeniem funkcjonalności usługi. Ponadto cofnięcie zgody powinno być równie łatwe jak jej wyrażenie[211], co w praktyce może prowadzić do fragmentaryzacji systemu analitycznego oraz obniżenia skuteczności mechanizmów detekcji nadużyć.

Masowe oparcie analizy danych behawioralnych na zgodach klientów może zatem prowadzić do paradoksalnej sytuacji, w której instrument zaprojektowany w celu zwiększenia bezpieczeństwa stanie się operacyjnie nieskuteczny w wyniku wycofania zgód przez istotną część użytkowników.

6.4.1.3. Profilowanie oraz decyzje zautomatyzowane

Analityka danych behawioralnych bardzo często spełnia definicję profilowania w rozumieniu art. 4 pkt 4 RODO. Jeżeli na jej podstawie dochodzi do podjęcia działań takich jak blokada rachunku, podwyższenie poziomu uwierzytelnienia, wstrzymanie transakcji lub odmowa realizacji określonej operacji, należy rozważyć, czy nie mamy do czynienia z decyzją opartą wyłącznie na zautomatyzowanym przetwarzaniu, wywołującą skutki prawne lub w podobny sposób istotnie wpływającą na osobę, której dane dotyczą (art. 22 ust. 1 RODO)[212].

W takim przypadku administrator zobowiązany jest do zapewnienia co najmniej[213]:

- prawa do uzyskania interwencji człowieka,
- prawa do wyrażenia własnego stanowiska,
- prawa do zakwestionowania decyzji.

Dodatkowo, zgodnie z zasadą przejrzystości (art. 5 ust. 1 lit. a RODO), bank powinien w sposób zrozumiały przedstawić logikę działania systemu oraz znaczenie i przewidywane konsekwencje takiego przetwarzania[214]. W praktyce rodzi to napięcie pomiędzy wymogiem transparentności a koniecznością ochrony skuteczności systemów antyfraudowych. Wreszcie, ze względu na skalę oraz potencjalne ryzyko naruszenia praw i wolności osób fizycznych, wdrożenie systemów analizy behawioralnej w bankowości co do zasady wymaga przeprowadzenia oceny skutków dla ochrony danych (DPIA) zgodnie z art. 35 RODO[215].

6.4.2. PSD2 – silne uwierzytelnianie klienta a wykorzystanie analizy danych behawioralnych

Wykorzystanie analizy danych behawioralnych w bankowości należy rozpatrywać nie tylko przez pryzmat ochrony danych osobowych, lecz również w kontekście obowiązków regulacyjnych wynikających z dyrektywy PSD2 oraz towarzyszących jej regulacyjnych standardów technicznych (RTS SCA). Ramy te determinują sposób, w jaki instytucje finansowe mogą konstruować mechanizmy uwierzytelniania i zarządzania ryzykiem transakcyjnym. Zgodnie z art. 97 dyrektywy 2015/2366 (PSD2) dostawcy usług płatniczych są zobowiązani do stosowania silnego uwierzytelniania klienta (*Strong Customer Authentication – SCA*) w sytuacjach obejmujących m.in. dostęp do rachunku płatniczego online, inicjowanie

209 Art. 6 ust. 1 lit. f RODO; motyw 47 RODO.

210 Art. 4 pkt 11 oraz art. 7 RODO.

211 Art. 7 ust. 3 RODO.

212 Art. 22 ust. 1 RODO.

213 Art. 22 ust. 3 RODO.

214 Art. 13 ust. 2 lit. f oraz art. 14 ust. 2 lit. g RODO.

215 Art. 35 RODO.

elektronicznych transakcji płatniczych oraz czynności mogące wiązać się z ryzykiem nadużycia[216]. SCA, zgodnie z art. 4 pkt 30 PSD2, opiera się na wykorzystaniu co najmniej dwóch elementów należących do kategorii: wiedza (coś, co użytkownik wie), posiadanie (coś, co użytkownik posiada) oraz cecha indywidualna (coś, czym użytkownik jest)[217]. Regulacyjne standardy techniczne przyjęte w rozporządzeniu delegowanym 2018/389 (RTS SCA) doprecyzowują wymogi dotyczące niezależności elementów uwierzytelniania oraz ich odporności na przejęcie[218].

W tym kontekście dane behawioralne nie stanowią odrębnej kategorii normatywnej, lecz mogą funkcjonować jako:

- element wspierający ocenę ryzyka transakcji (*transaction risk analysis – TRA*),
- dodatkowa warstwa bezpieczeństwa wzmacniająca mechanizm SCA,
- narzędzie ciągłego uwierzytelniania (*continuous authentication*) w trakcie trwania sesji.

RTS SCA przewidują możliwość odstąpienia od stosowania silnego uwierzytelniania w przypadku niskiego poziomu ryzyka transakcji, pod warunkiem, że dostawca usług płatniczych stosuje zaawansowane mechanizmy monitorowania i analizy ryzyka[219]. Dane behawioralne mogą odgrywać kluczową rolę w tym procesie, umożliwiając dynamiczną ocenę spójności zachowania użytkownika z jego profilem historycznym. W praktyce oznacza to wykorzystanie sygnałów takich jak typowe wzorce korzystania z aplikacji, sposób interakcji z urządzeniem czy tempo realizacji operacji jako elementów modelu oceny ryzyka. Z perspektywy regulacyjnej istotne jest jednak, aby[220]:

- model analizy ryzyka był udokumentowany,
- poziom wskaźników oszustw (*fraud rates*) mieścił się w progach określonych w RTS,
- system był zdolny do wykazania skuteczności ex post w ramach nadzoru.

Brak spójności pomiędzy architekturą modelu behawioralnego a wymogami RTS może prowadzić do zakwestionowania przez organ nadzoru spełnienia przesłanek odstępstwa od SCA. W konsekwencji, bank naraża się na ryzyko regulacyjne, obejmujące konieczność modyfikacji systemu lub ograniczenie stosowania uproszczonych procedur uwierzytelniania.

Wykorzystanie danych behawioralnych w modelu ciągłego uwierzytelniania stanowi rozwinięcie klasycznego paradygmatu SCA, który zakłada punktowy moment uwierzytelnienia. W modelu *continuous authentication* tożsamość użytkownika jest weryfikowana w sposób dynamiczny przez cały czas trwania sesji. Z punktu widzenia PSD2 rozwiązanie to może wzmacniać bezpieczeństwo systemu płatniczego, jednak rodzi kilka napięć regulacyjnych. Po pierwsze, mechanizm taki nie może zastępować formalnych wymogów SCA tam, gdzie są one obligatoryjne. Po drugie, nadmierna automatyzacja reakcji systemu (np. natychmiastowa blokada transakcji bez jasnych kryteriów) może prowadzić do nieproporcjonalnych ograniczeń w dostępie do środków finansowych. W tym kontekście istotne znaczenie ma także obowiązek informacyjny wobec użytkownika. Chociaż PSD2 nie nakłada bezpośrednio tak szczegółowych wymogów transparentności jak RODO, konstrukcja relacji z klientem oraz zasada uczciwości i przejrzystości świadczenia usług płatniczych implikują konieczność odpowiedniego poinformowania o stosowanych mechanizmach bezpieczeństwa[221]. Nadmierna „niewidoczność" systemu analitycznego może z jednej strony wzmacniać jego skuteczność operacyjną, z drugiej jednak generować ryzyko reputacyjne w przypadku sporów dotyczących odmowy realizacji transakcji.

Podstawowe ryzyka prawne w obszarze PSD2 można zatem sprowadzić do trzech płaszczyzn:

- Ryzyko niespełnienia wymogów RTS SCA – jeżeli model behawioralny jest traktowany jako element analizy ryzyka, lecz nie spełnia kryteriów skuteczności i mierzalności określonych w regulacyjnych standardach technicznych.
- Ryzyko nieproporcjonalnej ingerencji w dostęp do środków – w przypadku automatycznych decyzji ograniczających realizację transakcji bez odpowiedniego mechanizmu weryfikacji.

216 Art. 97 PSD2.

217 Art. 4 pkt 30 PSD2.

218 Rozporządzenie delegowane Komisji (UE) 2018/389 z 27.11.2017 r. uzupełniające dyrektywę 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych, bezpiecznych, otwartych standardów komunikacji (RTS SCA).

219 Art. 18–20 RTS SCA (Transaction Risk Analysis).

220 Tamże.

221 Zasady ogólne przejrzystości i rzetelności świadczenia usług płatniczych w PSD2, w szczególności art. 52–58 PSD2.

- Ryzyko reputacyjne i nadzorcze – wynikające z braku jasnego osadzenia systemu w architekturze zarządzania ryzykiem oraz niewystarczającej dokumentacji modelu.

W konsekwencji analiza danych behawioralnych nie powinna być traktowana jako alternatywa dla wymogów PSD2, lecz jako element komplementarny wobec SCA i TRA, osadzony w formalnie udokumentowanym systemie zarządzania ryzykiem operacyjnym. Tylko wówczas możliwe jest pogodzenie innowacyjności technologicznej z rygorami regulacyjnymi właściwymi dla sektora usług płatniczych.

6.4.3. DORA oraz analiza danych behawioralnych w świetle zarządzania ryzykiem ICT oraz obowiązków dokumentacyjnych

W przeciwieństwie do RODO i PSD2, które koncentrują się odpowiednio na ochronie danych osobowych oraz bezpieczeństwie uwierzytelniania, rozporządzenie DORA oraz dyrektywa NIS2 osadzają analizę danych behawioralnych w szerszym kontekście odporności operacyjnej i zarządzania ryzykiem ICT. W tym ujęciu kluczowe znaczenie ma nie tyle sama dopuszczalność przetwarzania danych, ile zdolność instytucji finansowej do wykazania, że wdrożony model analityczny jest elementem systemowego, udokumentowanego i proporcjonalnego mechanizmu zarządzania ryzykiem.

DORA ustanawia jednolite wymogi dotyczące cyfrowej odporności operacyjnej sektora finansowego. Zgodnie z art. 6–15 DORA podmioty finansowe są zobowiązane do ustanowienia kompleksowych ram zarządzania ryzykiem ICT, obejmujących identyfikację, ochronę, wykrywanie, reagowanie i odzyskiwanie po incydentach[222]. System analizy danych behawioralnych – w szczególności wykorzystywany do wykrywania przejęć kont, nadużyć płatniczych czy anomalii w zachowaniu użytkownika – może zostać zakwalifikowany jako element mechanizmów detekcji incydentów oraz monitorowania zagrożeń. W tym kontekście staje się on częścią infrastruktury bezpieczeństwa ICT, a nie wyłącznie narzędziem biznesowym. Z perspektywy DORA kluczowe znaczenie mają trzy obszary:

- Formalne osadzenie modelu w strukturze zarządzania ryzykiem – system analityczny powinien być jednoznacznie przypisany do kategorii ryzyk (np. *fraud risk*, *cyber risk*) oraz objęty procesem regularnej oceny skuteczności[223].
- Dokumentacja i audytowalność modelu – instytucja musi być w stanie wykazać logikę działania systemu, zakres wykorzystywanych danych, sposób aktualizacji modeli oraz procedury reagowania na błędne klasyfikacje[224].
- Testowanie odporności operacyjnej – w określonych przypadkach systemy o istotnym znaczeniu dla bezpieczeństwa operacyjnego mogą podlegać testom penetracyjnym i testom odporności cyfrowej (*TLPT – Threat-Led Penetration Testing*)[225].

Brak formalnej integracji modelu analizy behawioralnej z ramami zarządzania ryzykiem ICT może prowadzić do sytuacji, w której nawet skuteczny technologicznie system zostanie uznany za niezgodny z wymogami regulacyjnymi z powodu niedostatecznej dokumentacji lub braku nadzoru zarządczego.

Istotnym elementem DORA jest także reżim dotyczący zarządzania ryzykiem związanym z podmiotami trzecimi świadczącymi usługi ICT (art. 28–44 DORA)[226]. W praktyce, wiele banków korzysta z zewnętrznych dostawców rozwiązań analityki behawioralnej. W takim przypadku instytucja finansowa zobowiązana jest do:

- przeprowadzenia oceny ryzyka przed zawarciem umowy,
- zapewnienia odpowiednich klauzul umownych dotyczących dostępu do danych i audytu,
- monitorowania ciągłości działania dostawcy.

Niedostateczna kontrola nad modelem dostarczanym przez zewnętrznego vendora może prowadzić do powstania tzw. ryzyka „czarnej skrzynki", w którym bank nie posiada pełnej wiedzy o logice działania systemu, a jednocześnie ponosi pełną odpowiedzialność regulacyjną.

222 Art. 6–15 DORA.

223 Art. 6 ust. 1–3 DORA.

224 Art. 11 i 13 DORA.

225 Art. 26–27 DORA.

226 Art. 28–44 DORA.

W świetle DORA kluczowym zagadnieniem staje się dokumentacja modeli analitycznych. Obejmuje ona w szczególności:

- opis źródeł danych i ich kategorii,
- architekturę modelu oraz logikę decyzyjną,
- procedury aktualizacji i walidacji,
- metody monitorowania skuteczności i poziomu błędów (*false positives*/*false negatives*),
- procedury reagowania na incydenty.

Dokumentacja ta pełni podwójną funkcję: umożliwia zarządzanie ryzykiem wewnętrznym oraz stanowi materiał dowodowy w przypadku kontroli nadzorczej.

Na gruncie DORA analiza danych behawioralnych przestaje być wyłącznie zagadnieniem ochrony danych osobowych lub mechanizmem zwiększającym bezpieczeństwo transakcji. Staje się ona elementem systemowego zarządzania ryzykiem ICT oraz komponentem infrastruktury odporności operacyjnej. Podstawowe ryzyka regulacyjne obejmują:

- brak formalnego osadzenia modelu w strukturze zarządzania ryzykiem,
- niewystarczającą dokumentację i audytowalność systemu,
- niedostateczną kontrolę nad dostawcami zewnętrznymi,
- nieproporcjonalność wdrożonych środków bezpieczeństwa.

W konsekwencji, instytucja finansowa powinna traktować system analizy danych behawioralnych jako element architektury zgodności regulacyjnej (*compliance architecture*), a nie wyłącznie narzędzie technologiczne.

6.4.4. AI Act oraz kwalifikacja systemów analityki behawioralnej jako systemów wysokiego ryzyka

Wejście w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji (AI Act) zasadniczo zmienia kontekst regulacyjny wykorzystania analityki behawioralnej w sektorze bankowym. O ile RODO koncentruje się na ochronie danych osobowych, a PSD2 i DORA na bezpieczeństwie operacyjnym i uwierzytelnianiu, o tyle AI Act wprowadza autonomiczny reżim oceny ryzyka systemów sztucznej inteligencji, niezależny od podstawy przetwarzania danych czy sektora działalności[227]. W konsekwencji kluczowym pytaniem nie jest już wyłącznie to, czy analiza danych behawioralnych jest zgodna z zasadami ochrony danych, lecz czy wdrożony system spełnia kryteria kwalifikujące go jako system AI wysokiego ryzyka.

Zgodnie z art. 3 AI Act system AI oznacza system oparty na maszynie, zaprojektowany do działania z pewnym stopniem autonomii, który – na podstawie danych wejściowych – generuje wyniki takie jak przewidywania, rekomendacje lub decyzje wpływające na środowisko fizyczne lub wirtualne[228].

W praktyce bankowej modele analizy behawioralnej:

- wykorzystują techniki uczenia maszynowego,
- generują predykcje dotyczące poziomu ryzyka,
- klasyfikują zachowania jako typowe lub anomalne,
- mogą inicjować działania (np. dodatkową weryfikację, blokadę transakcji).

W zdecydowanej większości przypadków spełniają zatem definicję systemu AI w rozumieniu rozporządzenia.

AI Act wprowadza podejście oparte na klasyfikacji ryzyka. Zgodnie z art. 6 w zw. z załącznikiem III systemy AI wykorzystywane w obszarze dostępu do podstawowych usług prywatnych oraz oceny zdolności kredytowej osób fizycznych mogą zostać zakwalifikowane jako systemy wysokiego ryzyka[229].

W kontekście sektora finansowego system analityki behawioralnej może zostać uznany za wysokiego ryzyka w szczególności wtedy, gdy:

- wpływa na dostęp do rachunku bankowego,
- determinuje możliwość realizacji transakcji,
- uczestniczy w procesach oceny wiarygodności klienta,
- stanowi element automatycznego podejmowania decyzji o istotnych skutkach.

227 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13.06.2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (AI Act).

228 Art. 3 AI Act.

229 Art. 6 w zw. z załącznikiem III AI Act.

Nawet jeżeli system nie podejmuje decyzji kredytowych sensu stricto, lecz służy do wykrywania nadużyć, może zostać objęty reżimem wysokiego ryzyka, jeżeli jego działanie wpływa na możliwość korzystania z usług finansowych.

Zakwalifikowanie systemu analityki behawioralnej jako systemu wysokiego ryzyka powoduje nałożenie na dostawcę lub użytkownika szeregu obowiązków regulacyjnych, w tym:

- Obowiązek ustanowienia systemu zarządzania ryzykiem (art. 9 AI Act) – obejmującego identyfikację, analizę i ograniczanie ryzyk przez cały cykl życia systemu[230].
- Wymogi dotyczące jakości danych (art. 10) – dane treningowe, walidacyjne i testowe muszą być odpowiednie, reprezentatywne i wolne od nadmiernych uprzedzeń[231].
- Dokumentacja techniczna (art. 11) – obejmująca szczegółowy opis architektury systemu, logiki działania, parametrów i ograniczeń[232].
- Rejestrowanie zdarzeń (*logging*) (art. 12) – umożliwiające odtworzenie procesu decyzyjnego[233].
- Zapewnienie nadzoru człowieka (art. 14) – system nie może działać w sposób całkowicie autonomiczny bez możliwości interwencji[234].
- Ocena zgodności przed wprowadzeniem do obrotu lub oddaniem do użytku (art. 43)[235].

Z perspektywy banku oznacza to konieczność traktowania systemu analityki behawioralnej jako elementu regulowanego produktu, a nie wyłącznie narzędzia wspierającego bezpieczeństwo.

6.4.5. Kontekstowość dopuszczalności przetwarzania danych biometrycznych i behawioralnych

Analiza ryzyk regulacyjnych związanych z wykorzystaniem danych behawioralnych w bankowości wymaga uwzględnienia praktyki organów nadzorczych. Szczególne znaczenie ma w tym kontekście stanowisko Prezesa Urzędu Ochrony Danych Osobowych dotyczące stosowania danych biometrycznych w procesach przeciwdziałania praniu pieniędzy (AML), w którym organ zakwestionował możliwość oparcia przetwarzania na art. 9 ust. 2 lit. g RODO, wskazując na brak spełnienia przesłanki proporcjonalności oraz niewystarczające gwarancje ustawowe[236].

Stanowisko to stanowi przykład materializacji ryzyk, o których mowa w poprzednich podrozdziałach – w szczególności ryzyka nadmiernego rozszerzania zakresu przetwarzania danych szczególnych kategorii bez wyraźnej podstawy normatywnej oraz bez odpowiednich zabezpieczeń proceduralnych. Organ nadzorczy podkreślił, że samo istnienie obowiązku ustawowego w obszarze AML nie oznacza automatycznie dopuszczalności przetwarzania danych biometrycznych jako środka jego realizacji. Konieczne jest bowiem wykazanie, że zastosowanie takiego rozwiązania jest niezbędne, proporcjonalne oraz oparte na wyraźnych gwarancjach prawnych.

Należy jednak zauważyć, że stanowisko UODO zostało sformułowane w odniesieniu do konkretnego kontekstu regulacyjnego oraz określonego modelu wykorzystania biometrii – jako narzędzia identyfikacji w procesie weryfikacji klienta na potrzeby obowiązków AML. Analiza ta nie może być automatycznie przenoszona na wszystkie formy przetwarzania danych behawioralnych w systemach tożsamości cyfrowej.

Kluczowe znaczenie ma bowiem rozróżnienie funkcjonalne pomiędzy:

- wykorzystaniem biometrii jako podstawowego mechanizmu jednoznacznej identyfikacji osoby,
- zastosowaniem danych behawioralnych jako elementu wspierającego ocenę ryzyka, wykrywanie anomalii lub eskalację zabezpieczeń.

230 Art. 9 AI Act.

231 Art. 10 AI Act.

232 Art. 11 AI Act.

233 Art. 12 AI Act.

234 Art. 14 AI Act.

235 Art. 43 AI Act.

236 M. Krasińska, Odpowiedź na pismo Związku Banków Polskich do Ministerstwa Finansów z 21 stycznia 2023 r. dotyczącym przetwarzania wizerunku biometrycznego osób na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124 ze zm.), DPNT.023.179.2025.WL.PM, UODO, Departament Prawa i nowych Technologii, Wydział Legislacji, Warszawa 2025.

W pierwszym przypadku mamy do czynienia z bezpośrednim przypisaniem tożsamości do konkretnej osoby przy użyciu danych mogących stanowić szczególną kategorię danych osobowych. W drugim – dane behawioralne mogą pełnić funkcję sygnału ryzyka, który nie prowadzi do jednoznacznej identyfikacji, lecz do oceny prawdopodobieństwa nadużycia lub konieczności zastosowania dodatkowego uwierzytelnienia.

Różnica ta ma istotne znaczenie z perspektywy zasady proporcjonalności (art. 5 ust. 1 lit. c RODO) oraz oceny wpływu na prawa i wolności osób, których dane dotyczą[237]. Automatyczne utożsamienie każdego wykorzystania danych behawioralnych z przetwarzaniem danych biometrycznych w rozumieniu art. 9 RODO prowadziłoby do nadmiernego rozszerzenia reżimu szczególnych kategorii danych, niezależnie od rzeczywistej funkcji systemu.

Zarówno praktyka organów nadzorczych, jak i konstrukcja przepisów unijnych wskazują, że dopuszczalność stosowania danych biometrycznych lub behawioralnych nie ma charakteru generalnego, lecz zależy od kontekstu normatywnego oraz przyjętych gwarancji ochronnych.

W sektorach regulowanych, takich jak usługi płatnicze czy infrastruktura finansowa, projektodawca unijny expressis verbis dopuszcza stosowanie zaawansowanych mechanizmów bezpieczeństwa, pod warunkiem ich osadzenia w ściśle określonych ramach proceduralnych (np. PSD2, DORA). Oznacza to, że legalność takich rozwiązań jest uwarunkowana:

- istnieniem wyraźnej podstawy sektorowej,
- spełnieniem wymogów proporcjonalności,
- zapewnieniem nadzoru człowieka,
- prowadzeniem odpowiedniej dokumentacji i oceny ryzyka.

Stanowisko UODO potwierdza zatem nie tyle generalny zakaz stosowania danych biometrycznych, ile konieczność szczegółowej, kontekstowej analizy dopuszczalności przetwarzania. W praktyce oznacza to, że każdorazowo należy zbadać:

1) cel przetwarzania oraz jego niezbędność,

2) zakres danych i ich funkcję w systemie,

3) dostępne alternatywne środki mniej ingerujące w prywatność,

4) poziom zabezpieczeń technicznych i organizacyjnych.

Szczególne znaczenie ma wskazane wyżej rozróżnienie pomiędzy wykorzystaniem biometrii jako narzędzia identyfikacji a jej zastosowaniem jako mechanizmu wspierającego ocenę ryzyka lub eskalację zabezpieczeń.

W modelu identyfikacyjnym dane biometryczne pełnią funkcję podstawowego identyfikatora, a ich przetwarzanie bezpośrednio wpływa na status prawny jednostki (np. uznanie tożsamości, dostęp do rachunku). W modelu wspierającym dane behawioralne mogą służyć jedynie do podwyższenia poziomu uwierzytelnienia (np. wymuszenie dodatkowego czynnika SCA), bez samodzielnego rozstrzygania o dostępie do usługi.

Różnica ta wpływa na ocenę:

- intensywności ingerencji w prywatność,
- zakresu stosowania art. 9 RODO,
- konieczności uzyskania zgody,
- proporcjonalności środka w świetle celu.

Z perspektywy systemów tożsamości cyfrowej oznacza to, że nie każde wykorzystanie danych behawioralnych powinno być kwalifikowane w ten sam sposób. Kontekst funkcjonalny oraz architektura systemu mają znaczenie normatywne.

Stanowisko UODO w sprawie przetwarzania danych biometrycznych w procesach AML stanowi ważny sygnał ostrzegawczy dla sektora finansowego. Jednocześnie nie może być traktowane jako uniwersalny precedens wyłączający możliwość stosowania danych behawioralnych w innych konfiguracjach technologicznych.

Legalność takich rozwiązań nie ma charakteru abstrakcyjnego ani generalnego. Jest ona funkcją:

- celu przetwarzania,
- struktury systemu,
- poziomu ingerencji w prawa jednostki,
- istnienia wyraźnych gwarancji ustawowych i proceduralnych.

W konsekwencji kluczowym zadaniem instytucji finansowych nie jest rezygnacja z analityki behawioralnej, lecz zaprojektowanie jej w sposób, który uwzględnia zróżnicowanie funkcjonalne zastosowań

237 Art. 5 ust. 1 lit. c oraz art. 9 RODO.

oraz osadza system w jasno określonym kontekście normatywnym. Dopiero takie podejście pozwala pogodzić wymogi bezpieczeństwa cyfrowego z zasadami ochrony danych osobowych oraz standardami proporcjonalności.

Rozdział 7. Kierunki rozwoju i rekomendacje

7.1. Możliwości integracji biometrii behawioralnej z nowymi technologiami (AI, blockchain, zero trust)

7.1.1. Wprowadzenie

Wraz ze wzrostem skali i wyrafinowania cyberataków na sektor finansowy – od przejęć kont (ATO), przez oszustwa socjotechniczne, po zautomatyzowane kampanie fraudowe – widać coraz wyraźniej, że klasyczne, statyczne mechanizmy uwierzytelniania przestają wystarczać. Hasła, kody SMS czy kody jednorazowe są łatwe do wyłudzenia, sklonowania albo przechwycenia[238].

Biometria behawioralna, rozumiana jako ciągła analiza charakterystycznych dla danego użytkownika wzorców zachowania (np. dynamika pisania na klawiaturze, sposób korzystania z myszy czy telefonu), jest jedną z prób odpowiedzi na te wyzwania. W połączeniu z rozwiniętymi algorytmami sztucznej inteligencji (AI), technologią blockchain i architekturą *zero trust* może stać się filarem nowoczesnego, adaptacyjnego systemu bezpieczeństwa.

W niniejszym podrozdziale przedstawiono potencjał takiej integracji, związane z nią ryzyka oraz wyzwania regulacyjne. Omówiono także przykłady wdrożeń oraz wnioski praktyczne – zarówno z perspektywy technicznej, jak i organizacyjnej oraz prawnej.

7.1.2. Biometria behawioralna i AI

Współczesne systemy biometrii behawioralnej praktycznie nie istnieją bez sztucznej inteligencji. To właśnie algorytmy uczenia maszynowego i głębokie sieci neuronowe „uczą się" typowego sposobu korzystania z systemów bankowych przez konkretnego użytkownika. AI pozwala wykrywać subtelne zmiany, które trudno byłoby wychwycić za pomocą prostych reguł[239].

Analizowany może być m.in.:

- tempo i siła naciskania klawiszy,
- płynność, przyspieszenie i drobne korekty ruchów kursora,
- sposób trzymania telefonu, sposób interakcji ekranem,
- charakterystyczne przyspieszenia urządzenia mobilnego.

Na tej podstawie system może w tle, bez angażowania użytkownika, stale weryfikować, czy z konta korzysta właściwa osoba. Atutem AI jest adaptacyjność – modele mogą dostosowywać się do zmian zachowania (np. ktoś pisze wolniej, bo ma kontuzję dłoni), jeśli tylko proces ciągłego douczania jest prawidłowo zaprojektowany.

Wprowadzenie AI do systemów biometrii behawioralnej nie jest jednak wolne od problemów. Kluczowe są dwie grupy zagadnień:

- **Przejrzystość i wyjaśnialność (XAI).** Modele typu „czarna skrzynka" trudno jest wytłumaczyć klientowi, a tym bardziej regulatorowi. Tymczasem unijny AI Act wymaga, aby instytucje finansowe potrafiły pokazać, w oparciu o jakie przesłanki system podjął decyzję (np. odrzucił transakcję lub zażądał dodatkowego uwierzytelnienia). To wymusza inwestycję w rozwiązania zwiększające interpretowalność modeli – choćby w formie dodatkowych warstw raportujących główne czynniki wpływające na decyzję.
- **Jakość i stronniczość danych (bias).** Modele uczone na niepełnych lub „jednostronnych" danych mogą dyskryminować określone grupy

238 ENISA, ENISA Threat Landscape Finance Sector. January 2023 to June 2024, 2025.

239 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), EUR-Lex.

użytkowników, generować więcej fałszywych alarmów dla niektórych urządzeń czy typów zachowań. Dlatego konieczne jest trenowanie na zróżnicowanych danych (różne urządzenia, systemy operacyjne, grupy demograficzne), monitorowanie zjawisk typu *data drift*, regularna walidacja modeli w ramach procesów *Model Risk Management*.

7.1.3. Biometria behawioralna i blockchain

Blockchain kojarzy się przede wszystkim z niezmiennością zapisów i ich rozproszonym charakterem. W kontekście biometrii behawioralnej te cechy można wykorzystać m.in. do zapewnienia integralności danych i ich odporności na manipulacje[240].

Jednym z kierunków badań jest utrwalanie nie samych danych behawioralnych, lecz ich kryptograficznych „odcisków" (np. skrótów/hashy wektorów cech lub wyników scoringu) w sposób zapewniający integralność i rozliczalność. Taki efekt można osiągnąć zarówno poprzez standardowe mechanizmy kryptograficzne (hashowanie, podpisy cyfrowe, bezpieczne repozytoria audytowe, kwalifikowane znaczniki czasu), jak i, w wybranych scenariuszach, poprzez rejestry rozproszone. Kluczowe jest jednak, aby rozwiązanie nie zwiększało ryzyka korelacji i identyfikowalności użytkownika oraz nie utrwalało danych w sposób nieodwracalny.

W scenariuszu otwartej bankowości (*Open Banking*) umożliwia to stronom trzecim weryfikację autentyczności profilu behawioralnego bez dostępu do danych wrażliwych. Dodatkowo można łączyć to z kryptograficznymi mechanizmami typu *zero-knowledge proof*, aby potwierdzić, że dany użytkownik spełnia określone warunki, nie zdradzając szczegółów jego zachowania.

7.1.4. Biometria behawioralna i zero trust

Model *Zero Trust* opiera się na założeniu „never trust, always verify" – nie zakłada się zaufania ani do użytkownika, ani do urządzenia, nawet jeśli są już zalogowani. Każde żądanie dostępu traktowane jest jako potencjalnie podejrzane i wymaga ponownej oceny[241].

Biometria behawioralna bardzo naturalnie wpisuje się w tę filozofię, ponieważ:

- umożliwia ciągłe uwierzytelnianie w trakcie całej sesji,
- pozwala wykryć przejęcie sesji po zalogowaniu (np. przejęcie tokenu sesyjnego),
- może stanowić sygnał wyzwalający tzw. *step-up authentication* – dodatkową weryfikację, gdy coś w zachowaniu odbiega od normy.

W organizacjach przechodzących na pracę zdalną i usługi w chmurze takie podejście staje się standardem. Gartner wskazuje ciągłą autentykację jako jeden z filarów nowoczesnych architektur bezpieczeństwa. Przykład wdrożeniowy TypingDNA podkreśla, że kluczowe w Zero Trust jest „zabezpieczenie tego, co dzieje się pomiędzy punktami kontrolnymi", a więc właśnie monitorowanie użytkownika po logowaniu.

Integracja biometrii behawioralnej z systemami klasy EDR/XDR, SIEM oraz modułami UEBA (*User and Entity Behavior Analytics*) pozwala łączyć anomalie w zachowaniu użytkownika z innymi sygnałami (np. nietypowy ruch sieciowy, nowe urządzenie, nieoczekiwana lokalizacja). Dzięki temu decyzje o dostępie mogą być bardziej kontekstowe i dynamiczne: obniżanie wymagań wobec użytkownika, gdy ryzyko jest niskie oraz natychmiastowe zaostrzenie uwierzytelnienia lub izolacja sesji przy wysokim ryzyku.

7.1.5. Podsumowanie

Połączenie biometrii behawioralnej z AI, blockchain i architekturą zero trust tworzy propozycję nowej generacji zabezpieczeń w bankowości cyfrowej – rozwiązań, które działają w czasie rzeczywistym, są trudne do obejścia, a dla klienta pozostają w dużej mierze niewidoczne.

240 Lu Zhou, Abebe Diro, Akanksha Saini, Shahriar Kaisar, Pham Cong Hiep: Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities, Journal of Information Security and Applications, Volume 80, 2024, 103678.

241 NIST, SP 800-207 Zero Trust Architecture, 2020.

Z perspektywy regulacyjnej ten kierunek jest spójny z PSD2 i RTS SCA, wpisuje się w wymogi DORA i NIS2, a przy odpowiednim podejściu do zarządzania ryzykiem AI może być zgodny także z AI Act[242].

Prawdziwym wyzwaniem staje się nie tyle sama technologia, co sposób jej wdrożenia, tak aby był zrealizowany z poszanowaniem prywatności, przejrzystości i zaufania klientów.

7.2. Perspektywy rozwoju w bankowości cyfrowej i Open Finance

Współczesna bankowość cyfrowa funkcjonuje w środowisku o wysokim i dynamicznie zmieniającym się poziomie ryzyka. Tradycyjne mechanizmy uwierzytelniania, oparte na czynnikach wiedzy i posiadania, zostały istotnie wzmocnione przez wprowadzenie Silnego Uwierzytelniania Klienta (*Strong Customer Authentication – SCA*) na mocy dyrektywy PSD2, które wymusiło stosowanie modelu wieloskładnikowego. Należy jednak odróżnić formalny model SCA – mający charakter punktowy (np. przy logowaniu lub autoryzacji transakcji) – od szerszych mechanizmów monitorowania ryzyka stosowanych operacyjnie przez banki. W praktyce instytucje finansowe od dawna wykorzystują silniki oceny ryzyka oraz systemy monitoringu transakcyjnego, w tym w obszarze kart płatniczych, które analizują zachowanie użytkownika w czasie rzeczywistym również po uwierzytelnieniu. Ograniczenie polega więc nie na braku monitorowania, lecz na tym, że formalna konstrukcja SCA nie obejmuje ciągłej weryfikacji tożsamości w trakcie całej sesji użytkownika. W tym kontekście rośnie znaczenie rozwiązań umożliwiających bardziej adaptacyjne i kontekstowe podejście do bezpieczeństwa.

To właśnie w czasie pomiędzy logowaniem a zakończeniem sesji dochodzi dziś do wielu najpoważniejszych incydentów: przejęć sesji, ataków typu Man-in-the-Browser oraz manipulacji socjotechnicznych, w których uwierzytelniony użytkownik – działając pod wpływem nacisku, strachu czy błędnych informacji – sam zleca nieuprawnione przelewy.

Odpowiedzią na te problemy jest biometria behawioralna: technologia, która pozwala weryfikować tożsamość w sposób ciągły i niemal niewidoczny dla użytkownika (tzw. *passive authentication*), poprzez analizę jego charakterystycznego sposobu korzystania z urządzeń elektronicznych.

W kontekście nadchodzących regulacji PSD3 i PSR (*Payment Services Regulation*), a także inicjatywy FIDA (*Financial Data Access*), sektor bankowy musi z jednej strony uszczelnić systemy transakcyjne, z drugiej – zapewnić wysoką jakość doświadczeń użytkownika (UX) w coraz bardziej otwartym ekosystemie danych[243]. Biometria behawioralna, działająca „w tle", jawi się jako element łączący te, na pierwszy rzut oka sprzeczne, cele: pozwala ograniczyć „tarcie" po stronie klienta, nie rezygnując z wysokiego poziomu bezpieczeństwa.

7.2.1. Analiza rynku

Rynek rozwiązań biometrii behawioralnej dojrzewa i obejmuje zarówno dostawców lokalnych, jak i globalnych.

Polska jest ciekawym polem do obserwacji: z jednej strony to rynek bardzo innowacyjny technologicznie, z drugiej – objęty restrykcyjną interpretacją przepisów o ochronie danych osobowych. Największą barierą wdrożeniową dla biometrii behawioralnej pozostaje niepewność co do podstawy prawnej jej stosowania. Rynek rozwiązań biometrii behawioralnej dojrzewa i obejmuje zarówno dostawców lokalnych, jak i globalnych.

Odpowiedzią na część tych wyzwań są działania podejmowane wspólnie przez sektor. Biuro Informacji Kredytowej, po przejęciu spółki Digital Fingerprints, zbudowało międzybankową platformę biometrii behawioralnej[244].

W modelu tym klient, który zgodził się na analizę swojego zachowania w jednym banku, może być chroniony również w innych instytucjach uczestniczących w systemie. Nie chodzi tu o zastąpienie wewnętrznych mechanizmów monitorowania stosowanych przez poszczególne banki, lecz o rozszerzenie perspektywy analizy ryzyka na poziom międzyin-

242 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA), EUR-Lex.

243 European Commission, Financial data access and payments package (PSD3, PSR, FIDA), 28 June 2023.

244 Biuro Informacji Kredytowej, informacja prasowa, Biuro Informacji Kredytowej inwestuje w polski fintech (włączenie Digital Fingerprints do grupy BIK), 1 June 2022.

stytucjonalny. Wzorzec behawioralny użytkownika – odpowiednio zanonimizowany lub reprezentowany w formie sygnału ryzyka – może stać się elementem współdzielonej wiedzy o zagrożeniach. Ma to szczególne znaczenie w walce z tzw. „kontami mułów", czyli rachunkami masowo zakładanymi w różnych bankach przez te same grupy przestępcze. Mechanizmy działające wyłącznie w obrębie jednej instytucji mogą nie wykrywać powtarzalnych schematów występujących w skali sektora.

7.3. Rekomendacje dla instytucji finansowych

W dobie inżynierii społecznej i zautomatyzowanych ataków (np. Account Takeover), sektor bankowy musi zmienić podejście do tożsamości cyfrowej. Odpowiedzią jest biometria behawioralna – analiza tego, jak użytkownik wchodzi w interakcję z systemem, a nie tylko tego, co wie lub posiada. To już nie science-fiction, ale praktyczna konieczność i standard, do którego zmierza rynek. Poniżej przedstawiamy kompleksowe rekomendacje dla instytucji finansowych, obejmujące architekturę systemów, kwestie prawne oraz czynnik ludzki.

Należy odejść od binarnego podziału na użytkownika „zalogowanego" i „niezalogowanego". W modelu Zero Trust (*„never trust, always verify"*) zaufanie do sesji jest dynamiczne. Biometria behawioralna powinna działać w tle przez cały czas (*Continuous Authentication*). Jeśli system wykryje anomalię – np. nagłą zmianę dynamiki pisania sugerującą bota lub zdalny pulpit – powinien automatycznie wymusić dodatkową weryfikację tożsamości[245] (ang. *step-up authentication*), a w skrajnych przypadkach przerwać sesję.

Analiza behawioralna musi być zintegrowana z innymi systemami, w tym z systemami antyfraudowymi (walidacja krzyżowa sygnałów, np. czy ruch telefonu z akcelerometru zgadza się z danymi GPS) oraz systemami klasy IAM i NAC (wewnętrznie, w banku, biometria może weryfikować, czy pracownik korzystający z wrażliwych danych to na pewno uprawniona osoba, a nie ktoś, kto przejął odblokowaną stację roboczą).

Warto również obserwować potencjał technologii blockchain w zapewnianiu niezmienności logów biometrycznych oraz w modelach suwerennej tożsamości (*Self-Sovereign Identity*), gdzie wzorzec behawioralny mógłby być jednym z kryptograficznie potwierdzonych kluczy użytkownika.

W celu zapewnienia porównywalności i audytowalności rozwiązań niezbędne jest przyjęcie spójnych metryk skuteczności (m.in. FAR/FRR) oraz jednoznacznych definicji pojęć stosowanych w analizie behawioralnej. Instytucje finansowe, które wdrożą te rozwiązania w sposób przemyślany i zgodny z wymogami regulacyjnymi, mogą zwiększyć swoją odporność operacyjną oraz ograniczyć koszty związane z nadużyciami.

W przyszłości profil behawioralny może stać się „przenaszalny", co oznacza, że klient korzystający z usług wielu podmiotów (banki, fintechy) w ramach otwartej bankowości, mógłby być weryfikowany przez jeden zaufany profil behawioralny. Wymaga to jednak stworzenia ram zaufania i standardów wymiany danych.

Wdrożenie biometrii behawioralnej to strategiczna inwestycja w odporność sektora finansowego. Dobrze zaprojektowany system – działający w tle, szanujący prywatność (*Privacy-by-Design*) i wspierany przez kompetentny personel – pozwoli zatrzeć granicę między bezpieczeństwem a wygodą użytkowania. Banki, które wdrożą te rozwiązania w sposób przemyślany, zyskają przewagę konkurencyjną, będąc gotowe na wyzwania bankowości jutra.

245 European Banking Authority, Q&A, Use of behavioural data for SCA (odwołanie do EBA Opinion EBA-Op-2019-06), 16 Nov 2020.

Rozdział 8. Zakończenie

8.1. Podsumowanie wniosków

Raport jednoznacznie wskazuje, że klasyczne podejście oparte na jednorazowym akcie logowania nie odpowiada współczesnym zagrożeniom. Przejęcia kont i sesji coraz częściej następują *po poprawnym uwierzytelnieniu*, co ujawnia strukturalne ograniczenia tradycyjnych metod i wymusza odejście od modelu „login–hasło–SCA" jako jedynego punktu kontroli. Raport potwierdza też ewolucję uwierzytelniania w kierunku architektur wielowarstwowych, opartych na bieżącej ocenie ryzyka, kontekstu i zachowania użytkownika w trakcie całej sesji. Zaufanie w relacji bank–klient nie ma już charakteru jednorazowego, lecz dynamiczny i adaptacyjny. Ponadto autorzy konsekwentnie podkreślają, że dane behawioralne nie powinny być traktowane jako środek jednoznacznej identyfikacji osoby, lecz jako mechanizm wykrywania anomalii, nadużyć i zagrożeń cyberbezpieczeństwa. Takie ujęcie pozwala lepiej wpisać ich wykorzystanie w ramy interesu publicznego oraz zasad RODO, w tym minimalizacji i proporcjonalności danych. Ponadto największą wartość biznesową i bezpieczeństwa przynoszą wdrożenia, w których biometria behawioralna jest jednym z wielu sygnałów wejściowych do silnika ryzyka. Rozwiązania te pozwalają selektywnie uruchamiać silniejsze mechanizmy SCA tylko tam, gdzie faktycznie występuje podwyższone ryzyko, poprawiając jednocześnie UX i odporność systemów. Raport wskazuje na potrzebę wypracowania wspólnych słowników pojęć, metryk (np. FAR/FRR) oraz mechanizmów współdzielenia wiedzy o nowych wzorcach ataków pomiędzy bankami. W dłuższej perspektywie możliwe jest także pojawienie się „przenaszalnych" profili behawioralnych, co jednak wymaga ram zaufania i standardów wymiany danych na poziomie sektorowym. Autorzy konkludują, że biometria behawioralna stanowi inwestycję w odporność operacyjną sektora finansowego. Warunkiem sukcesu jest jednak projektowanie rozwiązań zgodnie z zasadą *privacy-by-design*, transparentność wobec klientów oraz odpowiednie kompetencje organizacyjne. Banki, które podejdą do tego w sposób systemowy, uzyskują realną przewagę konkurencyjną.

8.2. Odpowiedź na pytania badawcze

We wstępie raportu wskazano sześć pytań badawczych, oto one:

Q1. Jakie są kluczowe wyzwania uwierzytelniania klientów banku i jak są one osadzone w modelach zarządzania tożsamością?

Q2. Czym biometria behawioralna różni się od tradycyjnych metod biometrycznych i jakie ma zalety oraz ograniczenia w usługach finansowych?

Q3. Jakie cechy behawioralne są typowo wykorzystywane w bankowości i jak wygląda proces ich pozyskania oraz analizy?

Q4. W jaki sposób biometria behawioralna wspiera wykrywanie nadużyć oraz ciągłą ocenę ryzyka w czasie rzeczywistym?

Q5. Jakie są główne ryzyka etyczne i reputacyjne oraz jakie warunki są kluczowe przy użyciu danych behawioralnych?

Q6. Które kierunki rozwoju zastosowań nowych technologii są najbardziej perspektywiczne dla banków?

Na podstawie opracowanego raportu wypracowano odpowiedzi na wyżej wymienione pytania.

Odpowiadając na pytanie pierwsze, należy wskazać, że zasadnicze wyzwania uwierzytelniania klientów banku wynikają z dynamicznego charakteru bankowości cyfrowej oraz z faktu, iż przejęcie konta lub sesji nierzadko następuje już po poprawnym zalogowaniu. W konsekwencji podejście oparte na pojedynczym, punktowym akcie uwierzytelnienia ujawnia istotne ograniczenia i wymaga uzupełnienia o mechanizmy pozwalające oceniać wiarygodność użytkownika w toku całej sesji, z uwzględnieniem kontekstu działania oraz poziomu ryzyka związanego z wykonywanymi czynnościami. W raporcie napięcie to zostało osadzone w analizie ewolucji uwierzytelniania w kierunku modeli kontekstowych i atrybutowych, a także w tezie, że współczesne środowisko zagrożeń sprzyja przechodzeniu ku architekturze

wielowarstwowej, w której zaufanie w relacji bank–klient nie jest rozstrzygane jednorazowo, lecz podlega bieżącej weryfikacji. Jednocześnie analiza modeli zarządzania tożsamością wskazuje, że wybór architektury federacji tożsamości oraz modelu eIDAS/eIDAS2 współdecyduje o roli banku w ekosystemie oraz o dopuszczalnym zakresie środków kontrolnych. Modele wewnętrzne i usługowe porządkują rejestrację, logowanie oraz zarządzanie dostępem na dużą skalę, jednak z natury ograniczają przenoszalność tożsamości i relacyjność zaufania w środowiskach wielopodmiotowych.

W odniesieniu do pytania drugiego wypada podkreślić, że biometria behawioralna różni się od klasycznych metod biometrycznych przede wszystkim tym, iż nie opiera się na względnie stałej cesze fizycznej, lecz na sposobie interakcji użytkownika z systemem. Jej istota ma charakter probabilistyczny i kontekstowy, ponieważ nie sprowadza się do potwierdzenia "tożsamości" na podstawie niezmiennego wzorca, lecz do porównania zachowania obserwowanego w danej sesji z profilem odniesienia oraz do oceny stopnia zgodności i ryzyka. Umożliwia to wykorzystanie biometrii behawioralnej jako warstwy wspierającej uwierzytelnianie ciągłe, co stanowi odpowiedź na ograniczenia tradycyjnych mechanizmów punktowych w usługach finansowych. Wśród zalet należy wskazać możliwość wykrywania anomalii i nadużyć bez wprowadzania dodatkowych obciążeń po stronie klienta, a zatem przy zachowaniu użyteczności kanałów cyfrowych. Technika ta może wzmacniać bezpieczeństwo operacji, ograniczać skutki przejęć kont oraz wspierać przeciwdziałanie oszustwom. Zarazem wiąże się z ograniczeniami, do których należą nieusuwalne ryzyka błędów decyzyjnych, w tym fałszywych alarmów i przeoczeń, a także wyzwania audytowe, szczególnie w sytuacji wykorzystania metod uczenia maszynowego. W raporcie kwestie te powiązano z potrzebą wdrożenia mechanizmów walidacji i monitoringu jakości oraz przeciwdziałania stronniczościom danych, co warunkuje akceptowalność rozwiązania zarówno z perspektywy bezpieczeństwa, jak i zgodności regulacyjnej.

W kontekście pytania trzeciego należy zauważyć, że w bankowości najczęściej wykorzystywane są takie cechy behawioralne jak dynamika pisania na klawiaturze, wzorce ruchu kursora, sposób nawigacji po interfejsie, a także charakterystyki interakcji mobilnych, w tym gesty dotykowe oraz dane z czujników ruchu urządzenia. W ujęciu raportu istotne jest to, że są to sygnały powstające w sposób naturalny podczas korzystania z usług, które mogą być pozyskiwane pasywnie jako element kontekstu sesji. Zestaw takich cech pozwala konstruować profil użytkownika oraz identyfikować odstępstwa sugerujące przejęcie sesji, automatyzację działań bądź nienaturalny przebieg procesu. Proces pozyskania i analizy obejmuje rejestrację mikrozachowań po stronie aplikacji lub przeglądarki, następnie bezpieczne przekazanie danych do warstwy analitycznej, przetwarzanie wstępne, normalizację i ekstrakcję cech, a w dalszej kolejności – modelowanie oraz wyznaczenie miary ryzyka dla bieżącej sesji. Z perspektywy praktyki wdrożeniowej szczególne znaczenie ma fuzja sygnałów, rozumiana jako połączenie oceny behawioralnej z innymi danymi bezpieczeństwa i telemetrią w celu uzyskania decyzji kontekstowej, na przykład uruchomienia dodatkowego uwierzytelnienia lub wstrzymania operacji. Raport wiąże te etapy z opisem zastosowań w bankowości oraz z przykładami wykorzystania zachowań użytkownika w procesach zdalnych, w tym w ramach scenariuszy KYC.

Odnosząc się do pytania czwartego, należy wskazać, że biometria behawioralna wspiera wykrywanie nadużyć i ciągłą ocenę ryzyka poprzez monitorowanie spójności zachowania użytkownika z jego profilem odniesienia w czasie trwania sesji. Oznacza to odejście od wyłącznego polegania na poprawności logowania na rzecz obserwacji wzorców interakcji i identyfikacji anomalii mogących świadczyć o przejęciu konta, aktywności złośliwego oprogramowania, automatyzacji czynności albo wymuszonej aktywności użytkownika. W modelu przyjętym w raporcie przekłada się to na bieżące wyznaczanie miary ryzyka oraz dobór reakcji adekwatnej do poziomu zagrożenia, w tym podniesienie poziomu uwierzytelnienia, dodatkową weryfikację bądź przerwanie sesji. Efektywność tego podejścia wzrasta wraz z integracją z narzędziami wykrywania anomalii i z ekosystemem monitorowania, w szczególności – z systemami klasy SIEM oraz komponentami analitycznymi wspierającymi zarządzanie incydentami. Taka integracja umożliwia korelację sygnałów behawioralnych z innymi wskaźnikami ryzyka i prowadzi do bardziej wiarygodnej oceny zdarzenia, co ma szczególne znaczenie w obliczu nowych zagrożeń, takich jak przejęcia kont oraz ataki socjotechniczne. Raport akcentuje przy tym, że w wielu scenariuszach oszustw użytkownik pozostaje formalnie zalogowany, co czyni analizę behawioralną jedną z nielicznych warstw zdolnych do wykrywania subtelnych odchyleń w przebiegu sesji.

W odniesieniu do pytania piątego należy podkreślić, że ryzyka etyczne i reputacyjne związane z wykorzystaniem danych behawioralnych wynikają przede wszystkim z ciągłego charakteru monitorowania, który może zostać odebrany jako nadmierna ingerencja w prywatność, zwłaszcza gdy komunikacja z klientem jest nieczytelna i ogranicza się do formalnego wypełnienia obowiązku informacyjnego.

Ryzyko reputacyjne narasta również w sytuacji generowania błędnych alarmów, utrudnień w dostępie do konta lub nierównego traktowania użytkowników, wynikającego z jakości danych, różnic urządzeń oraz zróżnicowanych warunków korzystania z usług. W raporcie wskazano ponadto na problem rozliczalności i weryfikowalności działania narzędzi analitycznych, szczególnie wówczas, gdy decyzje operacyjne opierają się na złożonych modelach. Warunki odpowiedzialnego użycia danych behawioralnych obejmują zatem zapewnienie proporcjonalności i minimalizacji, jednoznaczne ograniczenie celu do bezpieczeństwa, wdrożenie środków ochrony danych na etapie projektowania oraz przeprowadzenie oceny skutków dla ochrony danych w sytuacjach, gdy przetwarzanie może generować wysokie ryzyko dla praw i wolności osób. Niezbędne pozostają również mechanizmy nadzoru nad modelem, walidacja jakości i monitorowanie zmian danych w czasie, a także transparentność rozumiana jako zdolność do przekazania klientowi sensu i skutków analiz behawioralnych, w szczególności odróżniająca ten cel od profilowania o charakterze marketingowym.

Udzielając odpowiedzi na pytanie szóste, należy wskazać, że najbardziej perspektywiczne kierunki rozwoju zastosowań nowych technologii w bankowości obejmują integrację biometrii behawioralnej z metodami sztucznej inteligencji, co sprzyja zwiększeniu skuteczności wykrywania anomalii i różnicowaniu reakcji w zależności od kontekstu ryzyka. Równocześnie raport akcentuje konieczność dojrzałego podejścia do zarządzania modelami, obejmującego kontrolę jakości danych, monitorowanie zmian profili w czasie oraz zapewnienie rozliczalności, ponieważ brak tych elementów może prowadzić do neutralizacji korzyści technologicznych przez ryzyka prawne i reputacyjne. Wysoki potencjał przypisuje się również architekturom *Zero Trust* i uwierzytelnianiu ciągłemu, w których zaufanie nie jest rozstrzygane jednorazowo, lecz podlega aktualizacji w świetle obserwacji przebiegu sesji, co odpowiada realiom przejęć kont oraz złożonych kampanii oszustw. Na poziomie ekosystemu finansowego raport wskazuje ponadto, że rozwój Open Finance i rosnąca interoperacyjność usług zwiększają znaczenie rozwiązań działających w tle, które podnoszą bezpieczeństwo bez pogarszania doświadczeń użytkownika, a jednocześnie mogą zostać powiązane z technologiami wzmacniającymi integralność i współdzielenie zaufania, w tym z rozwiązaniami opartymi na rozproszonych rejestrach.


BANK
PROGRAM
ANALITYCZNO
BADAWCZY