

RAPORT Z BADANIA

AKTUALNE WYZWANIA PRAWNE ZWIĄZANE Z ZASTOSOWANIEM SZTUCZNEJ INTELIGENCJI W POLSKIM SEKTORZE BANKOWYM

Sygn. PAB/WIB 8/2024



ISBN 978-83-965973-9-7

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

Stan prawny na 8 kwietnia 2024 r.



PROGRAM
ANALITYCZNO
BADAWCZY

O raporcie

Raport „**Aktualne wyzwania prawne związane z zastosowaniem sztucznej inteligencji w polskim sektorze bankowym**” został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Autorzy

Raport został opracowany przez zespół w składzie:

Dr hab. Krzysztof Koźmiński (red.) – Kierownik Zakładu Ekonomicznej Analizy Prawa, a także kierownik Centrum Oceny Skutków Regulacji oraz kierownik Podyplomowego Studium Zagadnień Legislacyjnych na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Radca prawny, partner zarządzający w kancelarii Jabłoński Koźmiński.

Prof. UW dr hab. Sławomir Żółtek – Prorektor ds. studentów i jakości kształcenia Uniwersytetu Warszawskiego, założyciel i pierwszy kierownik Centrum Badań nad Prawnymi Aspektami Technologii Blockchain działającego na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego.

Dr Michał Jabłoński – Doktor nauk prawnych, adiunkt w Katedrze Prawa i Postępowania Administracyjnego Uniwersytetu Warszawskiego. Adwokat, partner zarządzający w kancelarii Jabłoński Koźmiński.

Dr Colin W.P. Lewis – Specjalista w dziedzinie nauki o danych i ekonomii behawioralnej, data scientist z ponad 30-letnim doświadczeniem, uznawany za pioniera w społeczności sztucznej inteligencji, szczególnie w odniesieniu do globalnych finansów w bankach centralnych, publicznych i prywatnych.

Jan Czarnocki – Doktorant i stypendysta Marii Skłodowskiej-Curie w KU Leuven Centre for IT & IP Law. Zajmuje się badaniem prywatności i ochrony danych, koncentrując się na danych biometrycznych i zdrowotnych w kontekście IoT-AI, w ramach projektu Horizon 2020 Privacy Matters ITN.

Aleksander Leszczyński – Prawnik, doktorant w Katedrze Prawa Karnego Wydziału Prawa i Administracji Uniwersytetu Warszawskiego.

Michał Macidłowski – Prawnik, doktorant w Katedrze Prawa Karnego Wydziału Prawa i Administracji Uniwersytetu Warszawskiego.

Seweryn Sasin – Prawnik, doktorant w Szkole Doktorskiej Nauk Społecznych na UMK w Toruniu, przygotowuje rozprawę doktorską poświęconą wykorzystaniu sztucznej inteligencji w wydawaniu automatycznych aktów administracyjnych.

O programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie analizy zjawisk, tworzenia opracowań i porządkowania wiedzy w obszarach 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 wykorzystania ich wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz kreowania wartości dla klientów bankowości. PAB WIB kładzie duży nacisk na rozwój współpracy ze środowiskami akademickimi i eksperckimi, poszukując synergii w zakresie zainteresowań badawczych autorów oraz potrzeb rozwojowych sektora bankowego.

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 Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@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

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

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
www.pabwib.pl

Spis treści

	Streszczenie kierownicze	5
	1. Sztuczna inteligencja w bankowości. Wprowadzenie	8
	2. Doświadczenia polskie	10
	2.1. Wywiady pogłębione – kwestie metodologiczne	11
	2.2. Wywiady pogłębione: próba podsumowania i przykładowe odpowiedzi	11
	2.3. Przykłady rozwiązań inne niż wskazane przez respondentów	21
	2.4. Wnioski	35
	3. Przegląd doświadczeń zagranicznych	38
	3.1. Wprowadzenie	39
	3.2. USA	40
	3.3. UK	46
	3.4. Francja	49
	3.5. Niemcy	53
	3.6. Chiny	54
	3.7. Przykłady faktycznego zastosowania sztucznej inteligencji w bankowości światowej	56
	3.8. Wnioski z analizy komparatystycznej	57
	3.9. Rekomendacje dla projektodawców oraz prawodawców regulacji AI na podstawie analizy komparatystycznej	60
	4. Stan prawny: obecny oraz kierunki zmian legislacyjnych	62
	5. Podsumowanie wyników badań	85
	Załącznik. Scenariusz wywiadu z respondentami	92

Słowa kluczowe

Sztuczna inteligencja, AI, SI, bankowość, sektor bankowy, AI ACT, chatbot, robodoradztwo, cyberbezpieczeństwo, voicebot, biometria, automatyzacja, ryzyka, konsumenci, RODO, dane osobowe, proporcjonalność, wyjaśnialność, dyskryminacja, rynek finansowy, nadzór, regulacja, soft law, etyka, compliance, personalizacja, hiperpersonalizacja

Streszczenie kierownicze





Cel przeprowadzonego badania

Celem, który postawili sobie autorzy niniejszego raportu, było udzielenie odpowiedzi na pytania: na ile rozwiązania oparte o sztuczną inteligencję (dalej również jako: „AI” lub „SI”) są w praktyce aktualnie wykorzystywane w polskim sektorze bankowym, jak banki krajowe wypadają na tle doświadczeń zagranicznych, a także czy są przygotowane na poważne zmiany legislacyjne związane z wejściem w życie kompleksowej regulacji unijnej w postaci tzw. AI ACT.

Odbiorcy raportu

Raport powstał z myślą przede wszystkim o: podmiotach rynku finansowego (m.in. bankach, towarzystwach ubezpieczeń i emerytalnych), działających w obszarze tego rynku organach władzy publicznej, a także innych organów stosujących oraz stanowiących prawo.

Przedmiot analizy

Analizie poddano aktualnie stosowane rozwiązania przez polskie banki (korzystając m.in. z metody empirycznej, tj. wywiadów z respondentami-reprezentantami sektora bankowego, a także informacji dostępnych w domenie publicznej). Ponadto przeprowadzono – metodą komparatystyczną (prawoporównawczą) – weryfikację stanu prawnego w obszarze sztucznej inteligencji w kilku wybranych krajach (m.in. USA, Chiny, Francja, Niemcy). W końcu, stosując typową metodę badań prawnych (tzw. metodę formalno-dogmatyczną) zbadano rozwiązania obecne w AI ACT, sygnalizując towarzyszące regulacji wątpliwości oraz wyzwania.

Wnioski wynikające z badania

Przeprowadzone badania wykazały m.in., że polski sektor bankowy:

- ▶ jest świadomy wyzwania interdyscyplinarności, w tym zwłaszcza integracji perspektywy prawniczej z wiedzą technologiczną, związanego ze stosowaniem sztucznej inteligencji;
- ▶ deklaruje nie tylko najwyższą troskę o jakość wykorzystywanych mechanizmów bazujących na sztucznej inteligencji, jak i przekonanie, że pozostają one w zgodzie z obowiązującym prawem;

- ▶ minimalizuje ryzyka, unikając stosowania rozwiązań potencjalnie wątpliwych prawnie lub generujących niebezpieczeństwo roszczeń odszkodowawczych;
- ▶ postrzega sztuczną inteligencję jako szansę wsparcia i udoskonalenia dotychczasowych (tradycyjnych) procedur, w których kluczową rolę odgrywa realny człowiek;
- ▶ wykorzystuje aktualnie SI jako mechanizm „wspierający” procesy decyzyjne, nie zastępując, czy tym bardziej nie eliminując czynnika ludzkiego, a już z pewnością nie uchylając nadzoru pełnionego przez pracowników banku;
- ▶ prowadzi działalność edukacyjną na polu sztucznej inteligencji, skierowaną w pierwszej kolejności do pracowników banku, lecz również osób zewnętrznych, w tym konsumentów, klientów biznesowych, a nawet obywateli i przedsiębiorców niebędących klientami banku;
- ▶ wykorzystuje AI na bardzo szerokich i różnorodnych polach zastosowania;
- ▶ jest świadomy powagi zmian w otoczeniu prawno-regulacyjnym, związanych z AI ACT;
- ▶ jest, na tle innych państw Unii Europejskiej, zaawansowany technologicznie;
- ▶ trafnie identyfikuje (aktualne oraz przyszłe) kluczowe zagrożenia i ryzyka związane z AI;
- ▶ preferuje raczej twarde i precyzyjne regulacje w prawie powszechnie obowiązującym, zamiast *soft law* lub samoregulacji;
- ▶ wyraża obawy przed „przeregulowaniem” nowoczesnych technologii, w tym AI, w prawie unijnym, które – inaczej niż kraje azjatyckie lub USA – niekiedy przesadnie chroni konsumenta usług bankowych, ograniczając w ten sposób postęp technologiczny sektora bankowego.

Rekomendacje

Rekomenduje się permanentne monitorowanie, prowadzone zarówno z perspektywy indywidualnych banków, jak i organizacji zrzeszających banki, wchodzących w życie oraz planowanych zmian regulacyjnych w obszarze sztucznej inteligencji.



Ponadto, pozytywnie ocenić trzeba dotychczasowe wysiłki oraz zachęcić banki do dalszych działań na polu podnoszenia świadomości i edukacji w obszarze nowych technologii, kierowanych zarówno do pracowników, jak i społeczeństwa, w tym w szczególności klientów.

Zaleca się również dalsze ostrożne rozwijanie zastosowań w oparciu o technologię sztucznej inteligencji przez banki, respektując przy tym spełnianie obowiązków informacyjnych, zapobieganie niedyskryminacji oraz bezpieczeństwa użytkowników.

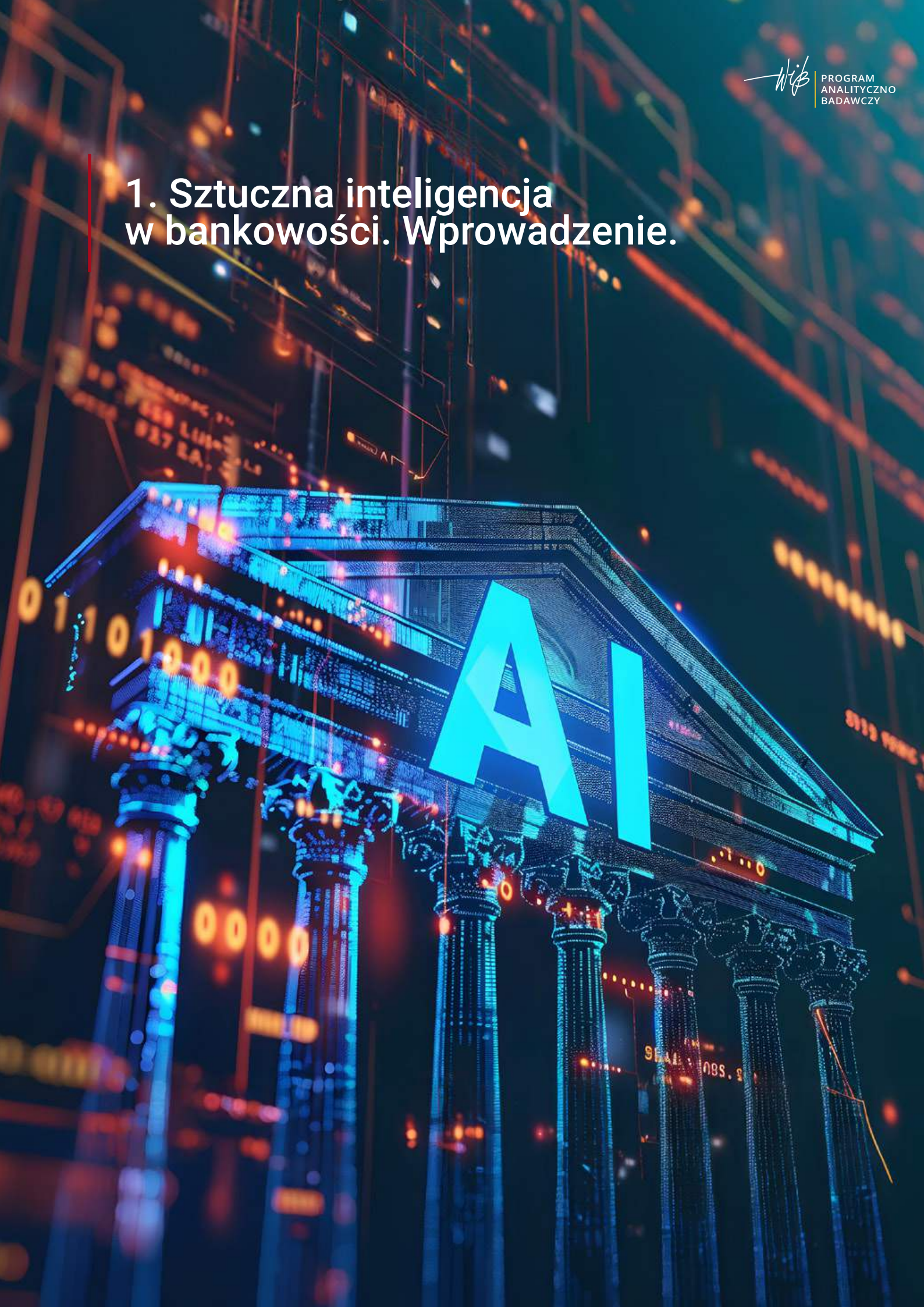
Rekomenduje się prowadzenie bieżącego dialogu pomiędzy instytucjami zaangażowanymi w nadzór nad rynkiem finansowym, a działającymi na nim przedsiębiorcami (w tym bankami) w celu wy-

pracowania optymalnych rozwiązań we wdrażaniu AI ACT.

Rozwiązaniem pożądanym jest też zaangażowanie instytucji państwowych oraz podmiotów sektora bankowego w finansowanie programów grantowych oraz innych inicjatyw, promujących rozwój sztucznej inteligencji oraz popularyzację wiedzy o niej.

Sugeruje się również intensyfikację współpracy banków z instytucjami nauki oraz ośrodkami badawczymi, co pozwoli nie tylko prowadzić wspólne projekty rozwojowo-badawcze, ale również pozyskiwać wsparcie eksperckie, umacniając status polskich banków jako nie tylko prężnych przedsiębiorców finansowych, lecz również dynamicznie rozwijających się firm technologicznych.

1. Sztuczna inteligencja w bankowości. Wprowadzenie.





Problematyce zastosowania sztucznej inteligencji w funkcjonowaniu podmiotów rynku finansowego, w tym zwłaszcza banków, a także związanych z tym wyzwań oraz ryzyk prawnych, poświęcono w ostatnim czasie wiele opracowań – w tym raportów eksperckich, publikacji naukowych, oficjalnych dokumentów instytucji publicznych oraz innych analiz prawno-ekonomicznych, zarówno zagranicznych¹, jak i polskich².

Celem, który postawili sobie autorzy niniejszego raportu było – zamiast powielania dotychczasowych analiz – udzielenie odpowiedzi na pytanie: na ile rozwiązania oparte na sztucznej inteligencji są w praktyce aktualnie wykorzystywane w polskim sektorze bankowym, jak banki krajowe wypadają na tle doświadczeń zagranicznych, a także czy przygotowane są na poważne zmiany legislacyjne związane z wejściem w życie kompleksowej regulacji unijnej w postaci tzw. AI ACT.

Dlatego też, inaczej niż w przypadku większości dostępnych obecnie opracowań, zdecydowaliśmy się na podjęcie dialogu z przedstawicielami polskiego sektora bankowego, tj. przeprowadzenie wywiadów pogłębionych z respondentami – reprezentantami środowiska finansowego, którzy dzieląc się własnymi doświadczeniami, przemyśleniami i przewidywaniami, prezentują oceny na temat zalet i wad nowoczesnej technologii (w tym zwłaszcza sztucznej inteligencji), formułują rekomendacje oraz postulaty *de lege ferenda* skierowane do prawodawcy oraz instytucji nadzorczych. Wywiady stanowią również dobrą okazję do zastanowienia się w jaki sposób promować sztuczną inteligencję wśród

konsumentów, zaznajamiać z nią obywateli, dostarczać impulsu przedsiębiorstwom technologicznym oraz podejmować cenną i efektywną współpracę z ośrodkami naukowymi. Zwłaszcza, że – jak pokazują badania – spora część polskiego społeczeństwa obawia się wykorzystywania sztucznej inteligencji w usługach powszechnych, wiążąc ją z niebezpieczeństwem niewłaściwego wykorzystania danych lub innych form cyberprzestępczości³. Lękom tym towarzyszą niepokoje związane z transakcjami bezgotówkowymi oraz ograniczeniem tradycyjnych form płatności⁴.

W niniejszym raporcie uwzględniliśmy dynamicznie zmieniające się otoczenie prawne, w tym zwłaszcza AI ACT, a także doświadczenia zagraniczne, będące nie tylko źródłem cennych inspiracji dla legislatorów i prawodawcy, lecz również samych instytucji finansowych, zdolnych na podstawie wiedzy komparatystycznej lepiej przewidywać potencjalne ryzyka, w konsekwencji zapobiegać im, łącząc walory technologii AI z koniecznym bezpieczeństwem.

Zastanawiamy się również, jako prawnicy doświadczeni w obszarze stanowienia prawa (stanowiący zdecydowaną większość zespołu autorów odpowiedzialnych za niniejszy raport), czy możliwe jest w ogóle legislacyjne objęcie i nadanie precyzyjnych ram prawnych zjawisku tak złożonemu oraz dynamicznie ewoluującemu, jak sztuczna inteligencja. Zwłaszcza, że wcale nie jest ono nowe, bo wprowadzone do obiegu jako pojęcie już w latach 50-tych poprzedniego stulecia⁵, a bardzo trudne do ujęcia w przepisach i niejednolicie rozumiane w różnych systemach prawnych.

1 Tytułem przykładu: *The Evident AI Innovation Report*, Evident Insights July 2023; *Impact of the New EU AI Regulation on Financial Sector Firms*, Clifford Chance, London 2021; European Commission, *Strategy for artificial intelligence*, europa.eu/en/policies/strategy-artificial-intelligence, dostęp: 11 sierpnia 2023 r.

2 Tytułem przykładu: *Raport Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości pt. „Zastosowanie sztucznej inteligencji w bankowości – szanse oraz zagrożenia”*, Warszawa 2022; *Sztuczna Inteligencja w Bankowości*, Uniwersytet SWPS-Związek Banków Polskich-Centrum Prawa Bankowego i Informacji, Warszawa 2020; D. Ślażyńska-Kluczek, *Sztuczna inteligencja – regulacje prawne, miejsce w polskim sektorze bankowym*, „Nauki Ekonomiczne”, 34/2021; M. Rojszczak, *Sztuczna inteligencja w innowacjach finansowych – aspekty prawne i regulacyjne*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny”, 2(9)/2020.

3 *Większość Polaków obawia się sztucznej inteligencji*, <https://www.bankier.pl/wiadomosc/Wiekszosc-Polakow-obawia-sie-sztucznej-inteligencji-8579020.html>, dostęp: 11 sierpnia 2023 r.

4 M. Jędrzejczak, *Całkiem bezgotówkowej Polski nie będzie – przynajmniej na razie*, <https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/calkiem-bezgotowkowej-polski-nie-bedzie-przynajmniej-na-razie/>, dostęp: 11 sierpnia 2023 r.

5 K. Maj, *Sztuczna inteligencja w prawdziwym banku [w:] Raport: Sztuczna inteligencja w bankowości*, Warszawa 2020, s. 10.

2. Doświadczenia polskie



2.1. Wywiady pogłębione: kwestie metodologiczne

Wywiady przeprowadzone zostały w oparciu o ankietę, zawierającą ujednolicony scenariusz rozmowy z respondentami (Załącznik nr 1 do niniejszego raportu), skonstruowany z pytań ogólnych, umożliwiających udzielanie swobodnych, otwartych odpowiedzi. Choć prośba o udział w badaniu skierowana została do ponad czterdziestu reprezentantów sektora bankowego (w tym wszystkich większych banków działających na terenie Rzeczypospolitej Polskiej) – przedstawicieli zarówno banków, jak i przedsiębiorstw technologicznych oraz firm doradczych współpracujących z bankami na polu wdrażania technologii sztucznej inteligencji – wytypowanych w oparciu o doświadczenie, wykonywane zadania oraz zajmowane stanowisko, w wywiadach udział wzięło finalnie dziesięcioro (10) respondentów: Krzysztof Semczuk (zastępca dyrektora ds. bankowości korporacyjnej i inwestycyjnej w banku PKO BP), Dawid Kin (dyrektor Biura Rozwoju Sztucznej Inteligencji w banku PKO BP), Radosław Kwiecień (członek zarządu Banku Gospodarstwa Krajowego), Katarzyna Góra (Head of Process Excellence w banku ING Bank Śląski), Karol Jaroszewski (dyrektor Studia Danych w Visa), Magdalena Lewandowska (dyrektor Departamentu Walidacji Modeli w Alior Bank), Łukasz Samborski (dyrektor Departamentu Zarządzania Ryzykiem Operacyjnym w Alior Banku), Rafał Kostowski (IT Area Lead I – AI w ING Bank Śląski), Jacek Trzyński (dyrektor Departamentu Nowych Technologii i Rozwoju w Banku Pekao S.A.) oraz Karina Daniel (dyrektor Biura AI w Departamencie Nowych Technologii i Rozwoju w Banku Pekao S.A.).

Wywiady były realizowane w okresie styczeń–marzec 2024 r.

Zdobyte w trakcie wywiadów informacje na temat stosowanych przez polskie banki rozwiązań, zostały ponadto uzupełnione i poszerzone o analizę źródeł dostępnych w domenie publicznej, w tym zwłaszcza strony internetowe banków, oficjalne dokumenty, wypowiedzi ich reprezentantów lub treści publikowane w social mediach. Wyniki tej analizy zaprezentowane zostały w podrozdziale 2.3. *Przykłady rozwiązań inne niż wskazane przez respondentów.*

2.2. Wywiady pogłębione: próba podsumowania i przykładowe odpowiedzi

Przed wszystkim dostrzec trzeba, że **każdy z respondentów-uczestników badania posiada wieloletnie doświadczenia zawodowe w sektorze bankowym, a także bogatą praktykę (choć zdobywaną z perspektywy wykonywania różnych obowiązków, wykształcenia i pracy w odmiennych jednostkach wewnętrznych banków) w procesie wdrażania nowoczesnych technologii, w tym sztucznej inteligencji, niejednokrotnie zdobywaną również poza krajowym sektorem bankowym, np.:**

„(...) od początku mocno wspierałem obszar AI, który dopiero się rodził, czyli w 2019 r. można powiedzieć już byłem w pełni zaangażowany w projekt wdrożenia voice botów w banku, a od dwóch lat jestem dyrektorem biura rozwoju sztucznej inteligencji, gdzie rozwijamy i voice boty i też inne rozwiązania wykorzystujące AI z zakresu wizji komputerowej, przetworzenia języka naturalnego i rozwiązywania innych problemów” [Dawid Kin].

„My naszą przygodę z machine-learningiem rozpoczęliśmy już ponad dziesięć lat temu, w obszarze modeli windykacyjnych. Pierwsze modele były bardzo proste, pozwalając nam przewidzieć przeterminowanie spłaty raty oraz to, czy klient w ogóle spłaci kwotę, którą wcześniej zadeklarował, tylko po pewnym czasie” [Katarzyna Góra].

Ponadto zasygnalizować trzeba, że **wszyscy respondenci podkreślali konieczność ścisłej współpracy pracowników banku odpowiedzialnych za sferę prawną i otoczenie regulacyjne (w tym compliance) ze specjalistami od technologii.** Innymi słowy: akcentowano potrzebę interdyscyplinarności i współdziałania ekspertów reprezentujących różne specjalizacje w procesie wdrażania oraz nadzorowania instrumentów bazujących na sztucznej inteligencji.

Niezależnie od udzielanych wypowiedzi, dość powiedzieć, że kilka wywiadów odbyło się „w parach” (np. Krzysztof Semczuk i Dawid Kin z banku PKO BP), tj. wypowiedzi prawników uzupełniane były przez osoby odpowiedzialne za infrastrukturę techniczną lub indywidualni respondenci deklarowali przygoto-



wywanie się do wywiadu poprzez wewnętrzne rozmowy w swoim banku z pracownikami o odmiennej specjalizacji. W tym sensie uzasadniona jest generalna teza, że **reprezentanci polskiego sektora bankowego świadomi są wyzwania interdyscyplinarności, w tym zwłaszcza integracji perspektywy prawniczej z wiedzą technologiczną, związanego ze stosowaniem sztucznej inteligencji.**

Niezależnie od reprezentowanej instytucji, profilu zawodowego i wykształcenia respondenta, **we wszystkich przeprowadzonych wywiadach akcentowano nie tylko najwyższą troskę o jakość wykorzystywanych mechanizmów bazujących na sztucznej inteligencji, ale również przekonanie, że pozostają one w zgodzie z obowiązującym prawem.** Co więcej, sygnalizowano wręcz, że – w razie wystąpienia najmniejszych choćby wątpliwości lub zastrzeżeń co do ich legalności – banki, jako instytucje zaufania społecznego oraz jedne z najściślej regulowanych przedsiębiorców, minimalizują ryzyko, unikając stosowania danego rozwiązania (lub stosując je w ramach testów wewnętrznych, pilotaży, symulacji albo wyłącznie pomocniczo i pod ścisłym nadzorem człowieka).

„(...) ogólnie sztuczna inteligencja w banku jest wykorzystywana od wielu lat, bo do predykcji sprzedaży – to jest naturalne wykorzystanie uczenia maszynowego i różnych algorytmów. Czyli cała predykcja sprzedaży pod kątem wyznaczania najlepszej oferty dla danego klienta, czy jakby próby zrozumienia, którym klientom warto zaproponować jakiś produkt i to się dzieje od lat. To jest naturalne. Oczywiście też kolejnym obszarem, takim dużym w banku, gdzie wykorzystywane jest uczenie maszynowe, jest obszar ryzyka, czyli próba częściowej oceny wniosków np. kredytowych w taki sposób abyśmy tej oceny mogli po prostu dokonywać szybciej, aby klient nie musiał czekać tak jak to było wiele, wiele lat temu, gdy każdy wniosek musiał być dokładnie oglądany z każdej strony i to człowiek podejmował każdą decyzję. Jako bank dążymy do tego, aby w tych sprawach, w których można i w których to jest uzasadnione, żeby po prostu ten udział modeli był jak najwyższy. Ale oczywiście zawsze w sposób totalnie zgodny z prawem i ze wszystkimi wymogami. Bo to też wiadomo, że jest obszar bardziej uregulowany i ta wytłumaczalność modeli też musi być zachowana i to są takie dwa obszary, w których to się po prostu rozwijało od dawna” [Dawid Kin].

„(...) sektor bankowy ma trudniej niż inne i to jest normalne, czyli mówimy o AI Act’ie, mówimy

o przepisach, ale no trzeba sobie powiedzieć, że gdybyśmy byli tylko spółką technologiczną bez tej licencji bankowej, to byśmy mieli już o wiele więcej rozwiązań zaimplementowanych. Mieliśmy bardzo szeroko wykorzystywaną generatywną sztuczną inteligencję i to naprawdę bardzo szeroko, ale jesteśmy bankiem i sektor bankowy na pewno ma to zadanie implementacji AI trochę trudniejsze, bo na przestrzeni lat, a to w obszarze zarządzania ryzykiem trzeba było być bardziej uważnym niż inne firmy, a to teraz w obszarze komunikacji, zawsze będziemy obciążeni pewnym ryzykiem, którym wiele firm nie jest, a które sprawia, że musimy trochę bardziej sztywno podchodzić do pewnych rzeczy i nie możemy ich implementować w tak szerokim zakresie w jakim byśmy tego chcieli, bo jednak też jesteśmy częściowo instytucją zaufania publicznego i to jest bardzo ważne; oprócz tego jesteśmy regulowani przez wiele innych przepisów, które po prostu mają wpływ też na implementację AI” [Dawid Kin].

„Jeśli chodzi o płatności i akurat tutaj w kontekście sztucznej inteligencji możemy się pochwalić tym, że jako pierwsza firma płatnicza globalnie zaczęliśmy stosować sieci neuronowe już w 1993 r. zaczęliśmy wykorzystywać sieci neuronowe do oceny ryzyka danej transakcji. Oczywiście zawsze naszą intencją było to, żeby zapewniać naszym partnerom biznesowym, ale też konsumentom, posiadaczom naszych kart absolutne bezpieczeństwo, jeśli chodzi o te transakcje. W związku z tym sztuczne inteligentne sieci neuronowe pozwalały nam oceniać, które transakcje mogą być transakcjami oszukańczymi i w zasadzie to jest czymś co, czym rzeczywiście się szcycimy. (...) ciągle rozwijamy od tych 30 lat. (...) ale oczywiście to nie jest jedyne wykorzystanie sztucznej inteligencji, które funkcjonuje w naszej organizacji” [Karol Jaroszewski].

„Sztuczna inteligencja i jej wykorzystanie w sektorze bankowym to obecnie gorący temat. Trwają dyskusje na temat potencjału jej generatywnej odłony, która definiuje wiele nowych kierunków zastosowań AI, ale również kładzie nacisk na aspekty regulacyjne, bezpieczeństwa oraz te dotyczące sfery etycznej. Jako bank musimy w sposób przemyślany decydować o tym, gdzie jest przestrzeń na efektywne wykorzystanie GenAI, a w których miejscach jej klasyczna odłona w pełni realizuje stawiane przed nami wymagania. Dobrym kierunkiem może być również testowanie rozwiązań własnych (dla odczytu

dokumentacji bankowej, analizy sentymentu, odsłuchów), których celem jest weryfikacja potrzeb banku, procesów oraz rozwiązań AI, budowa doświadczeń i kompetencji przed dalszym pójściem w rozwiązania rynkowe. Jako bank, którego głównym zadaniem jest dostarczanie jak najwyższej jakości produktów i usług dla naszych klientów koncentrujemy się na analizie i wdrażaniu rozwiązań, które udoskonalają standardy obsługi zapewniając jednocześnie jak największe bezpieczeństwo naszych klientów. Realizujemy te cele zarówno w obszarach automatyzacji obsługi klienta – boty, jak również w zaawansowanej analizie interakcji głosowych oraz tekstowych. Dotyczy to także szeroko rozumianych procesów związanych z zarządzaniem wiedzą, dzięki którym otwierają się nowe możliwości budowy rozwiązań nowoczesnych, efektywnych, zapewniających wyższą od dotychczasowej skuteczność działania. To kierunki, które zapewniają jeszcze lepszą jakość obsługi klienta, wspartą kompleksową i aktualizowaną na bieżąco wiedzą na jego temat. Aktywny rozwój funkcjonalności dostępnych w aplikacjach mobilnych w oparciu o zaawansowaną analitykę pozwala na ich personalizację pod kątem oferty ze względu na coraz szerszą i kompleksową analizę klienta (widok 360 stopni). Praca nad zaawansowanymi algorytmami, które umożliwią automatyczną analizę nastrojów oraz opinii na temat naszych produktów i usług to kolejny element budujący strategię banku aktywnie odpowiadającego na potrzeby swoich klientów. Wykorzystanie zaawansowanych algorytmów sztucznej inteligencji, w tym GenAI, w celu efektywnego zarządzania wiedzą w ramach organizacji i w kontaktach z klientem daje szansę na otwarcie nowych modeli obsługi zarówno klientów banku, jak i klientów wewnętrznych. Umiejętność czytania różnych kategorii dokumentów i danych, ich streszczanie, podsumowywanie, połączone z botami konwersacyjnymi, to szansa na zbudowanie nowej jakości obsługi, efektywnej, minimalizującej ryzyko błędów jakościowych w zakresie przetwarzania wiedzy o banku. Automatyzacja procesów obsługowych klientów dzięki wykorzystaniu technologii bot ze wsparciem generatywnej AI to szansa na istotne zwiększenie jakości działania tych rozwiązań, także w zakresie rozszerzenia kompetencji botów i skuteczności ich działania w bezpośrednim kontakcie z klientem banku, także wewnętrznym. Te kierunki wsparte rozwojem mechanizmów minimalizujących ryzyko nieuczciwych aktywności wobec banku i jego klientów stanowią integral-

ną część podejścia do strategii wykorzystania sztucznej inteligencji na kolejne lata. Sprawnie działająca instytucja, której celem jest gwarantowanie najwyższych standardów obsługi, musi optymalizować swoją pracę zarówno w bezpośrednim kontakcie z klientem, ale również wewnętrznie, słuchając głosu instytucji i odpowiadając na jej najważniejsze potrzeby. W tym celu warto efektywnie wykorzystywać właśnie potencjał AI” [Jacek Trzyński].

Jednocześnie, to właśnie zmiany stanu prawnego – zarówno otoczenia legislacyjnego, jak i wykładni prawa, prezentowanej w rozstrzygnięciach sądów, organów lub choćby stanowiskach instytucji publicznych (np. Komisji Nadzoru Finansowego) – charakteryzowane są jako jedna z największych potencjalnych przeszkód lub wręcz ryzyk związanych z zastosowaniem sztucznej inteligencji. W tym kontekście kilku respondentów wspomniało o historii kredytów indeksowanych i denominowanych do kursów walut obcych (zwłaszcza tzw. kredytów frankowych), które – analogicznie do wielu nowoczesnych technologii – nie budziły w przeszłości zastrzeżeń prawnych, uchodząc za nie tylko legalne, ale wręcz korzystne dla konsumenta i mało ryzykowne dla klientów, by po wielu latach stać się źródłem tysięcy sporów sądowych i gigantycznych strat finansowych:

„(...) chociażby kwestie konsumenckie i temat franków pokazują nam, że takie przewidywanie jest potrzebne, jednocześnie jest na ten moment bardzo trudne albo też niemożliwe, bo w momencie, w którym kredyty frankowe były udzielane (...) wymiana walut nie generowała takich obaw, żeby tych produktów nie wdrażać. Teraz się okazało, że to jest po prostu krytyczne ryzyko i dzisiaj po prostu tych produktów na rynku nie ma” [Krzysztof Semczuk].

Zdecydowana większość uczestników rozmów widzi sztuczną inteligencję jako szansę wsparcia i udoskonalenia dotychczasowych (tradycyjnych) procedur, w których kluczową rolę odgrywa realny człowiek. Podkreśla się tu m.in. szybkość prowadzonych operacji, oszczędność zasobów, permanentną dostępność tej technologii oraz możliwość jednoczesnej obsługi wielu klientów naraz. W tym sensie AI – na zasadzie synergii, ale jednocześnie pod nadzorem decydenta-pracownika banku – jest w stanie dostarczyć rozwiązań bardziej efektywnych, np. w zakresie przetwarzania dużej ilości danych lub podniesienia poziomu bezpieczeństwa.



„(...) szczególnie w zakresie bezpieczeństwa i tych procesach związanych z praniem pieniędzy, kontrolą transakcji podejrzanych i ich ścieżkami. To jest ewidentnie bardzo żmudna praca od strony człowieka, a dzisiejsze systemy oparte na technologiach, nazwę je tradycyjnymi, mają swoje duże luki do pokrycia i mają pewne ograniczenia. Na pokrycie tych ryzyk operacyjnych nowe technologie na pewno pozwalają” [Radosław Kwiecień].

Co oczywiste: **niektóre z zadań realizowanych na rzecz klienta, sztuczna inteligencja jest w stanie świadczyć permanentnie, nie okazując zmęczenia oraz bez potrzeby angażowania pracowników banku w dni wolne od pracy, nietypowe godziny, a równie pewnie i niezawodnie, jak realni ludzie zatrudnienie w banku.**

„(...) mamy też obszar, który rozpoczął się w 2019 r. jako praca, w 2020 r. zaczęliśmy wdrażać pewne rozwiązania i to jest obszar botów i tu sytuacja wygląda tak, że po kilku latach tej pracy, mamy 19 voice botów, które przeprowadziły łącznie już ponad 31 milionów rozmów z klientami, mamy asystenta głosowego w aplikacji IKO. To jest taki voice-chat bot, czyli można do niego pisać, można z nim rozmawiać i on jest w naszej aplikacji mobilnej, plus mamy masę botów telefonicznych, czyli na infolinii banku (...) i dalej nad tym pracujemy jako już taki ciągły rozwój, ciągle doskonalenie. Natomiast, oprócz tego powstał szereg innych rozwiązań z różnych obszarów, czyli my w tej chwili dzwoniemy czasami, przeprowadzamy miłą windykację z klientami, przypominamy im o zaległościach. Oprócz tego właśnie sugerujemy tam na infolinii ponad sto tematów, na które klient może uzyskać odpowiedź, ale nie tylko odpowiedź, bo jeżeli powie, że zgubił portfel, chce zastrzec kartę, to przeprowadzimy z nim taki proces od A do Z. Tak samo bot jest w stanie odblokować klientowi jakieś zablokowane kanały. Około 30% rozmów na naszej infolinii przychodzących, to są rozmowy, które po prostu nie wymagają udziału człowieka, więc to już jest taki wskaźnik dosyć mocny, a będziemy pracować nad tym, aby to było jeszcze lepsze. Oprócz tego weszliśmy w szereg botów, gdzie albo by nie mogły być wykonane te zadania przez człowieka albo trwałoby to dłużej, więc między innymi boty, które mają na celu zabezpieczenie finansów klienta, czyli dzwoniemy do niego, kiedy wykona podejrzaną transakcję kartą, gdy nasze systemy bezpieczeństwa tak stwierdzą, aby pytać czy to na pewno on, czy chce kartę zastrzec, czy odblokować. Dzwoniemy do niego,

kiedy składa jakieś wnioski kredytowe, które są dla nas o tyle ważne, że chcemy to już teraz potwierdzić, bo mieliśmy też szereg ataków na telefony klientów, gdzie przestępcy dzwonili i kazali instalować jakieś oprogramowanie i próbowali w ten sposób składać wnioski i przelewać środki na swoje konta. Wykryliśmy, że to jeden z takich kanałów, nad którymi nie mają kontroli, więc dużo takich działań dodatkowych i tych botów jest naprawdę 19 i będzie tego przybywać” [Dawid Kin].

„Jest jeden przykład flagowy, oczywisty, tzn. bank się chwali wdrożeniem voice botów i chat botów, które się nazywają „infoNina”. Bank w ostatnich trzech latach otrzymał pięć wyróżnień za to wdrożenie i to są voice boty, które przyjmują rozmowy przychodzące klientów do call center i to jest na modelach AI’owych, wewnętrznych oczywiście” [Łukasz Samborski].

„(...) dzięki zastosowaniu sztucznej inteligencji jesteśmy w stanie przewidywać ataki hakerskie i skuteczniej się przed nimi bronić” [Karol Jaroszewski].

Jak zaznacza Radosław Kwiecień z BGK: **obecnie możliwości oferowane przez sztuczną inteligencję są testowane i weryfikowane jako alternatywne względem dotychczasowych procedur, w których główną rolę odgrywał człowiek, poprzez porównanie wyników oraz identyfikowanie potencjalnych różnic:**

„(...) zaczynamy porównywać wyniki przy rozwiązywaniu jakichś konkretnych problemów (...) wykonujemy działania, które dzisiaj mamy w naszej procedurze, a też patrzymy w jaki sposób zachowałby się, jakie byłyby rezultaty i wyniki, jeżeli byśmy zastosowali w części elementów np. kredytowe, właśnie tę technologię” [Radosław Kwiecień],

co jest istotne zwłaszcza z uwagi na fakt, że **aplikacja może się mylić, prezentować wadliwe ustalenia powstałe na skutek zjawiska halucynacji AI.**

Respondent podkreśla jednak, że **niejednokrotnie nieprawidłowa prognoza sztucznej inteligencji spowodowana jest błędem ludzkim, efektem zaniedbań, popełnionych na wcześniejszym etapie, polegających przykładowo na wprowadzeniu niepełnych lub niewłaściwych danych:**

„(...) gros niestety elementów, które widzimy jako ryzyko operacyjne w ramach wdrażania tej tech-

nologii, to są błędy. Najczęstsze są to błędy powielane przez wcześniej właśnie przez interfejsy białkowe, interfejsy ludzkie, które wprowadzając pewne błędy, AI z tego korzysta, przekonując resztę, że nie – to przecież tak właśnie wygląda. Robienie błędów czy pewnych wręcz kreacji nieprawdziwych zdarzeń czy nieprawdziwych faktów czy kreowanie faktów, robienie alternatywnych rzeczywistości występuje w tej technologii. Natomiast, my sobie zdajemy sprawę z ułomności tych rozwiązań, które są czasem przez sztuczną inteligencję dostarczane” [Radosław Kwiecień].

Finalnie zatem, jak zapewnia Radosław Kwiecień, **AI pełni aktualnie jedynie „rolę wspierającą” procesy decyzyjne, nie zastępując, czy tym bardziej nie eliminując czynnika ludzkiego, a z pewnością już nie uchylając nadzoru pełnionego przez pracowników banku.**

Dawid Kin z banku PKO BP zwrócił uwagę na interesujący przykład zastosowania sztucznej inteligencji, jakim jest **udoskonalenie procesu ewaluacji jakości usług oraz wykorzystanie go do identyfikacji mankamentów i podniesienia ich poziomu w przyszłości.**

„(...) zaczęliśmy automatycznie analizować opinie naszych klientów o naszej aplikacji mobilnej, zaczęliśmy automatycznie analizować opinie klientów o naszych oddziałach i w ten sposób zapewniliśmy też naszym zespołom wewnętrznym takie potężne narzędzia, które sprawiają, że oni widzą przez ściany, czyli wcześniej dyrektor oddziału mógł lub nie mógł, chciał lub nie chciał czytać opinie na temat tego oddziału na mapach Google, ale nie był w stanie z tego wyciągnąć żadnych informacji oprócz przeczytania tych opinii i zastanowienia się czy coś można poprawić. Aktualnie jest tak, że na tej podstawie budujemy porównania z innymi bankami, budujemy porównania między naszymi jednostkami w ramach jakiegoś konkretnego regionu, miasta, więc to jest taka informacja zarządcza na podstawie, której każda placówka wie, w którym obszarze jeszcze musi się rozwinąć, bo automatycznie klasyfikujemy też te wszystkie opinie” [Dawid Kin].

Jacek Trzyński oraz Karina Daniel wskazują zarówno na zalety, jak i potencjalne mankamenty sztucznej inteligencji:

„Zalety wykorzystania sztucznej inteligencji w sektorze bankowym przynoszą korzyści zarówno dla instytucji finansowych, jak i dla klien-

tów. Po pierwsze, jedną z zalet jest możliwość automatyzacji wielu procesów. Dzięki AI banki mogą znacząco oszczędzać czas i zasoby poprzez zautomatyzowanie rutynowych zadań. Na przykład, wykorzystanie chatbotów w komunikacji z klientem pozwala na szybką obsługę wielu pytań i wątpliwości bez konieczności udziału pracowników. Ponadto, automatyczne przetwarzanie wniosków kredytowych czy podejmowanie decyzji biznesowych opartych na analizie danych może znacząco przyspieszyć finalizację procesu. Kolejną zaletą jest możliwość uzyskania precyzyjnej analityki danych. Dzięki zaawansowanym algorytmom AI banki mogą dokładnie analizować zachowania klientów, trendy rynkowe oraz funkcjonowanie wewnętrzne instytucji. Ta szczegółowa analiza pozwala na usprawnienie pracy pracowników różnych departamentów i lepsze zrozumienie potrzeb klientów, co umożliwia personalizację ofert oraz redukcję CHURN. Ważnym elementem jest także wykorzystanie baz wiedzy ułatwiających dostęp do szczegółowych informacji. Dzięki przechowywaniu i systematyzacji danych w bazach wiedzy, można szybko uzyskać dostęp do potrzebnych informacji.

Jednym z głównych ryzyk jest możliwość nieprawidłowego funkcjonowania systemów AI. Nieodpowiednio przetworzone dane mogą skutkować podejmowaniem błędnych decyzji. Dlatego też, konieczne jest zapewnienie odpowiednich zabezpieczeń danych oraz przejrzystości w stosowaniu algorytmów AI. Trwające obecnie prace nad przygotowaniem właściwych regulacji, które staną się podstawą do wypracowania standardów monitorowania systemów wykorzystujących AI to jeden z pierwszych kroków, jakie przyjdzie nam wykonać, aby stworzyć środowisko minimalizujące ryzyka, o których mowa powyżej. Jako banki będziemy budować nowe i rozszerzać istniejące kompetencje, aby być jak najlepiej przygotowanym do realizacji procesów wdrażania, utrzymania i rozwoju systemów opartych lub wykorzystujących AI” [Jacek Trzyński, Karina Daniel].

Warto odnotować, że respondenci mają świadomość towarzyszących sztucznej inteligencji obaw ze strony pracowników, zaniepokojonych zmianami na rynku pracy oraz nowoczesnymi technologiami, które w niedalekiej przyszłości zdolne będą zastąpić część personelu, prowadząc do redukcji etatów. Wątek ten podniósł m.in. Radosław Kwiecień, sygnalizując dość zaskakujące zjawisko, tj. sytuację, w której **z jednej strony pracownicy banku zgłaszają**

gotowość, ciekawość i wolę współpracy przy projektach angażujących sztuczną inteligencją, z drugiej zaś formułują lęki z tym związane:

„Tu już wchodzimy w aspekty zarówno prawne, ale też relacji pracowniczych (...) w dzisiejszych czasach pracownicy tych zespołów sami się wręcz zgłaszają, chcą pracować. Zadają sobie pytanie, czy to wyeliminuje naszą pracę, czy tam w jakiś sposób ograniczy naszą aktywność w organizacji” [Radosław Kwiecień].

W kwestii wpływu sztucznej inteligencji na stan zatrudnienia i podział ról w banku, **respondenci są raczej zgodni w kwestii zmiany obejmującej profil pożądanych pracowników oraz charakter wykonywanej przez nich pracy, która przesunie się bardziej na nadzór nad narzędziami sztucznej inteligencji, obejmującymi tak różne obszary, jak np. stosowanie prawa:**

„(...) nie chcę powiedzieć, że bardzo wiele osób straci pracę, tylko że praca wielu osób zostanie diametralnie zmieniona i będą musieli w inny sposób działać, być może współpracować z tymi rozwiązaniami, aby one zawsze działały poprawnie, ale to będzie olbrzymia rewolucja moim zdaniem w ciągu dwudziestu lat i potężna automatyzacja prawie wszystkich procesów w banku, ale też w wielu przypadkach automatyzacja wsparcia. (...). Ja wyobrażam sobie, że w przyszłości dział prawny, prawnicy to jest jakby jeden z przykładów, będzie miał o wiele łatwiejszą sprawę, bo będzie tak naprawdę takim strażnikiem tego czy jakieś tezy wysunięte przez tego typu modele są prawdziwe czy nie, aby to zweryfikować, ale nie będzie musiał pisać całej opinii od zera, tylko będzie mógł się naprawdę posiłkować potężnymi bazami, które też będą czerpać z doświadczenia innych. To jest rewolucja na każdym poziomie w ciągu dwudziestu lat moim zdaniem” [Dawid Kin].

Wszyscy respondenci deklarują działalność edukacyjną na polu sztucznej inteligencji, skierowaną w pierwszej kolejności do pracowników banku:

„patrząc na cały bank, mogę powiedzieć, że jesteśmy mocno zaawansowani w wykorzystywaniu sztucznej inteligencji, również w zakresie podnoszenia świadomości pracowników, bo razem z pionem Tech również stworzyliśmy taki program, który nazywa się Ai Trek i od czterech lat faktycznie edukujemy naszych pracowników” [Katarzyna Góra].

„Kolejnym istotnym aspektem jest edukowanie zarówno pracowników, jak i społeczeństwa na temat nowych technologii i sztucznej inteligencji. Te działania mogą pomóc w adaptacji do zmieniającego się krajobrazu technologicznego i zapewnić, że polski sektor bankowy pozostanie konkurencyjny na globalnym rynku. Im większa świadomość i zrozumienie AI, zasad jej działania, korzyści i zagrożeń wynikających z jej wykorzystywania, tym większa otwartość na wykorzystanie potencjału przy zachowaniu wymaganych zasad bezpieczeństwa” [Karina Daniel].

„Dość mocno edukujemy naszych pracowników, do tego edukujemy bardzo mocno data scientist’ów, mamy szeroki wachlarz kursów i szkoleń, dodatkowo umożliwiliśmy im również współpracę na przykład z uniwersytetami z zewnętrznymi ekspertami, a ponadto trzeci rok z rzędu zbieramy pomysły na zastosowanie sztucznej inteligencji w procesach operacyjnych w produktach bankowych, więc tutaj w zeszłym roku w ramach programu mamy zebrane ponad sto pomysłów, ponieważ nasi pracownicy również nie żyją w środowisku zamkniętym, więc wykorzystują różnego typu sztuczną inteligencję i dzielą się swoimi koncepcjami” [Katarzyna Góra].

„(...) my, jako Visa udostępniliśmy możliwość skorzystania z ChatGPT każdemu pracownikowi Visa na całym świecie (...) idea przyświecająca temu jest taka, że jeśli jesteśmy w stanie wygenerować jakąś wartość, którą potrzebujemy w sposób szybszy i prostszy, to czemu z tego nie skorzystać? (...) Oczywiście jest to wersja zamknięta chata, który jest oczywiście wdrożony na warunkach naszej organizacji. Jest to robione w sposób bezpieczny i oczywiście stosujemy zasady, które ustaliliśmy ogólnie jako organizacja, ale tak każdy pracownik Visa globalnie ma dostęp do ChatGPT. Dzięki temu może to oszczędzić czas, wykreować nowe efektywne rozwiązania na użytek naszej firmy” [Karol Jaroszewski].

Zdaniem większości respondentów, pewien **dystans, krytycyzm i ostrożność w aplikowaniu rozwiązań opartych o AI jest w stanie dać najlepszy efekt, równoważąc zalety z wadami i potencjalnymi ryzykami.**

„Jeżeli dokładnie przyjmiemy, że te mechanizmy są „najsłuszniejsze” i one mówią jedyną prawdę, to one nam stworzą olbrzymie problemy. Życie

w poziomie pewnego dystansu, kontroli i niepewności, jednak jest nomen omen bezpieczniejsze” [Radosław Kwiecień].

Podkreślić trzeba, że **wszyscy biorący udział w badaniu respondenci akcentują ostrożność i niezbędną zachowawczość we wdrażaniu rozwiązań opartych o sztuczną inteligencję, jako powody wskazując zarówno niedoskonałość dotychczasowej technologii, jak i ograniczenia prawne.**

„Przygotowujemy się bardzo ostrożnie do wdrażania tego typu rozwiązań też dlatego, że nikt nie daje do końca ręką takiej wiedzy panowania nad tym, w jaki sposób to działa, żeby mógł wyjaśnić jak pewne algorytmy działają. Zresztą to jest powszechna wiedza, że to narzędzie przy okazji ich twórców, żeby znać do końca reguły jak to działa. Nikt tego nie ma. Nikt tego nie wie, a drugi aspekt to są jednak kwestie prawne. Jestem przekonany, że najpierw muszą powstać uregulowania czy chociażby na poziomie Unii Europejskiej, prawa krajowego, regulatora sektora bankowego, który będzie to w pewien sposób kierunkował. Dzisiaj choćby nawet rozwiązania chmurowe, które wdrażamy w systemie są akceptowane ze strony KNF-u i w paru procesach notyfikacji tych przejść do chmury w pewnych elementach wykonujemy, bo przecież tam jest kwestia outsourcingu i prawo bankowe to reguluje i tutaj te rozwiązania muszą być zarządzane z poziomu banku, a nie pozostawione dostawcy usługi” [Radosław Kwiecień].

„Wszyscy działamy w tych samych ramach, na tym samym rynku. Wszystkich nas obowiązuje prawo bankowe i tajemnica bankowa w szczególności, a także wszyscy borykamy się z tymi samymi ograniczeniami. Nie mamy pełnej swobody wykorzystania rozwiązań sztucznej inteligencji” [Magdalena Lewandowska].

Jednocześnie respondenci podkreślają **potencjalne bardzo szerokie i różnorodne pola zastosowania AI przez banki:**

„z punktu widzenia back office na pewno widzę automatyzację prostych czynności takich, które są powtarzalne (...) na pewno widzę możliwość spersonalizowania oferty dla naszych klientów. I tutaj jest ten trend absolutnie widoczny, a tutaj coraz częściej wykorzystują sztuczną inteligencję. Ta personalizacja jest bardzo ważna. Dodatkowo jeżeli chodzi o sztuczną inteligencję, to na

pewno poprawa bezpieczeństwa naszych klientów i to zarówno modele przewencyjne, ale również te wykrywające, wykrywające pewnego typu anomalie. To tutaj na pewno w obszarze cyberbezpieczeństwa, antyfraud (...)” [Katarzyna Góra].

„(...) na przykład spersonalizowane skróty (personalizacja i kolejność ikon) w aplikacji mobilnej, czy też na przykład odpowiedzi dla klienta w kwestii preferowanych przez niego rozwiązań, odpowiedzi dotyczące cyklicznych płatności. Wiadomo, że w czasach, w których dużo różnych platform subskrybujemy – przydają się takie odpowiedzi: czy ta platforma streamingowa, czy inna platforma z audiobookami jest dla nas przydatna” [Rafał Kostowski].

Na pytanie, **czy zastosowanie sztucznej inteligencji w bankowości oznaczać będzie raczej stopniową ewolucję, czy jednak radykalną rewolucję w funkcjonowaniu banków, które były znane dotychczas – większość respondentów wskazało na ewolucję:**

„Wyda mi się, że to jest pewien postęp, którego my nie możemy uniknąć, ale ja bym powiedziała, że to nie jest rewolucja, tylko ewolucja (...) nie czujemy, że to jest olbrzymia rewolucja, tylko my po prostu zmieniamy nasze nawyki i zachowania i bank też uważam, że się dostosowuje do tego, co faktycznie się dzieje istnieje. Będziemy raczej uczyć się stosować pewne metody, które po prostu będą coraz bardziej dostępne” [Katarzyna Góra].

„Jak najbardziej, sztuczna inteligencja może zrewolucjonizować i w pewnym sensie już zmienia sektor bankowy, przynosząc nowe korzyści, ale również wyzwania. W zakresie personalizacji stosowanych usług dla klientów indywidualnych, firmowych, premium tworzymy lepiej dopasowane oferty budując coraz lepsze ich doświadczenie. Bank, za pomocą analizy danych, uczenia maszynowego oraz szerokiej gamy analiz predykcyjnych, będzie mógł lepiej zrozumieć indywidualne potrzeby klienta i w ten sposób proponować odpowiednie produkty – dostosowane kredyty, inwestycje, oszczędności. W ten sposób, biorąc pod uwagę indywidualne profile ryzyka i cele finansowe klienta, będziemy mogli wchodzić w interaktywną relację z klientem, bazując na obiektywnych analizach i obliczeniach. Na tym polu szczególnie może przydać się GenAI. Automatyzacja procesów i zwiększenie efektywności opera-

cyjnej pomoże przyspieszyć rutynowe i czasochłonne aktywności, tym samym zmniejszy to zapotrzebowanie na bezpośredni kontakt z pracownikiem CC i pozwoli im skupiać się na problemach klientów które wymagają bezpośredniego kontaktu z człowiekiem.

AI ze względu na swoją siłę przeliczeniową może szybko analizować przypadki naruszające bezpieczeństwo banku i klientów. W czasie rzeczywistym może dokonywać analizy wzorców transakcji, wykrywając potencjalne oszustwa finansowe, próby prania pieniędzy i inne nielegalne działania. Zważając na ilość dokonywanych dziennych transakcji, AI będzie mogło wykrywać podejrzane przypadki i przekazywać je do ludzkiego agenta w celu weryfikacji.

Dzięki rozwiązaniom typu knowledge management, które gromadzą dane różnych typów i formatów oraz odpowiednio te informacje klasyfikują, istnieje możliwość usprawnienia systemu pracy dla pracowników. W kontekście marketingu, AI pozwala na wytworzenie interaktywnego bota posiadającego zintegrowaną, lecz elastyczną osobowość. Wspiera to proces budowania marki banku innowacyjnego w świecie społecznym i internetowym. Fakt ten może stanowić zachętę dla potencjalnie nowych klientów do nawiązania relacji z taką instytucją finansową. AI jest zawsze dostępne i gotowe do pomocy, skutecznie działając może budować nową wartość dla instytucji finansowej.

AI może przyczynić się do zmiany dotychczasowych i rozwoju nowych modeli bankowych. Eksploracja tego jeszcze niezbyt obeznanego tematu, może przynieść korzyści pod względem usprawniania wewnętrznych procesów, ale i stworzenia całkowicie nowych usług i produktów, które mogłyby lepiej zaspokajać potrzeby klientów oraz odpowiadać na współczesne wyzwania rynkowe. Stosując etyczne rozwiązania AI, bankowość może stać się zdemokratyzowanym sektorem dla szerokiego spektrum klientów wspierając ich w migracji do kanałów zdalnych, tym samym wpływając na rolę oddziałów" [Jacek Trzyński i Karina Daniel].

Niemal wszyscy respondenci bardzo wysoko oceniają poziom zaawansowania technologicznego polskiego sektora bankowego, wskazując krajowe banki jako liderów na tle innych państw Unii Europejskiej.

„Polski sektor bankowy, podobnie jak w wielu innych krajach, dynamicznie rozwija się w obszarze wykorzystania nowoczesnych technologii i obecnie znajduje się w czołówce państw o najwyższym poziomie zaawansowania bankowości cyfrowej. Z raportów wynika, że około 30% procesów bankowych w Polsce jest już zautomatyzowanych, a liczba klientów korzystających z bankowości elektronicznej, mobilnej i transakcji online stale rośnie. Świadczy to o tym, że Polacy są otwarci na korzystanie z nowych technologii, jeśli tylko są one implementowane mądrze i z zachowaniem najwyższych standardów bezpieczeństwa. Jeśli chodzi o przykłady rozwiązań zagranicznych na pewno warto monitorować trendy związane z cyberbezpieczeństwem, migracją do chmury, wykorzystaniem generatywnej sztucznej inteligencji, ale raczej po to, by inspirować się, móc mądrze i bezpiecznie adaptować je do polskiej rzeczywistości” [Jacek Trzyński i Karina Daniel].

Przeprowadzone rozmowy wykazały też, że **respondenci są świadomi powagi zmian w otoczeniu prawnoregulacyjnym, związanym z AI ACT.**

„(...) jak czytam ten akt, to należy to rozwiązanie traktować jako system jednak dość wysokiego ryzyka, patrząc na to co zostało uregulowane w tym dokumencie. On się głównie opiera na elemencie związanym z zarządzaniem tożsamością. Tam elementy związane z zarządzaniem danymi wrażliwymi jak biometryka czy dane personalne, biologiczne, to jest jeden element, który na pewno jest istotny, a w biznesie bankowym bardzo istotny. Zresztą, już dzisiaj wykorzystywane są rozwiązania, w Polsce akurat niestety nie udane, ale rozwiązania biometryczne, które wracają teraz choćby do BIK-u i potwierdzanie transakcji fingerprintem, jest powrotem do tych rozwiązań jako dobre, bezpieczny background zarządzania tymi danymi. Kwestie, to co jest związane z RODO i wdrożenie tych rozwiązań RODO na pewno jest konieczne” [Radosław Kwiecień].

Z drugiej jednak strony – mimo bieżącego monitorowania stanu prawnego oraz prognozowania tego, w jaki sposób AI Act oraz towarzyszące mu zmiany przepisów wpłyną na ocenę prawną stosowanych narzędzi – **respondenci deklarują przyjmowanie przez ich banki postawy proaktywnej, mającej na celu minimalizację wszelkich ryzyk oraz eliminację rozwiązań potencjalnie niebezpiecznych, bo wątpliwych prawnie.** I tak np. reprezentanci PKO BP,

Krzysztof Semczuk i Dawid Kin, podkreślali troskę o „niedyskryminacyjny” charakter stosowanych w banku rozwiązań.

„Staramy się już teraz z tym działać, żeby nie czekać na AI Act, czyli jakby zwracanie uwagi na to, żeby te dane były różnorodne, którymi uczymy modele, co pozwala nam na to, że nie boimy się, że inaczej modele będą traktowały kobiety, mężczyzn, osoby młode, starsze. To jest pierwsze zagrożenie, czyli pewna automatyzacja podejmowania decyzji zawsze może prowadzić do tego, że źle przygotowany model przenosi na siebie cechy człowieka, który go przygotowywał. Jeżeli ta osoba ma pewne wyobrażenia na temat świata, a pracowała nad tym modelem sama no to zawsze jest jakaś szansa, że to będzie. To jest takie jedno z zagrożeń, natomiast ja bym powiedział, że ja widzę szereg zagrożeń takich, którymi łatwo zarządzić, które właśnie nadchodzący AI Act przewiduje” [Dawid Kin].

„W dniu 21 kwietnia 2021 r., Komisja Europejska przedstawiła wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii. Tworzenie, rozwój i wykorzystanie systemów sztucznej inteligencji będzie jednak wymagało uwzględnienia nie tylko przepisów AI Act lecz także szeregu innych, istniejących i aktualnie projektowanych regulacji prawnych. Analizy wewnętrzne wskazały na zależności pomiędzy AIA i wybranymi aktami prawnymi, przepisami i projektami aktów prawnych. W kontekście naszego sektora analiza odnosiła się również do wytycznych Urzędu Komisji Nadzoru Finansowego, mających znaczenie dla obszarów, w których sztuczna inteligencja może być lub jest wykorzystywana przez podmioty nadzorowane. W związku z dynamicznym rozwojem technologii, prawodawstwo dla sztucznej inteligencji staje się coraz bardziej istotne. Wprowadzenie regulacji prawnych dotyczących sztucznej inteligencji (AI) ma na celu zarówno ochronę praw jednostek, jak i zapewnienie odpowiednich ram prawnych dla innowacyjnych rozwiązań. W banku przygotowujemy się do wejścia AIA w życie projektując Politykę AI regulującą najważniejsze zastosowania AI. Wszystko to wskazuje na to, że regulacje prawne dotyczące sztucznej inteligencji w sektorze bankowym będą nadal ewoluować, aby sprostać wyzwaniom związanym z dynamicznym rozwojem technologii i będzie to proces, który na

stałe wpisze się w nasze życie. Tak jak już wcześniej wspomniano każda instytucja finansowa już teraz, w oparciu o istniejące regulacje, rozporządzenia – w tym AI Act – powinna pracować nad przygotowaniem polityk oraz standardów regulujących najważniejsze kwestie związane z wykorzystaniem technologii AI w zakresie wdrożenia, utrzymania i rozwoju systemów na niej opartych, zapewniając przy tym jak najwyższe bezpieczeństwo oraz poszanowanie norm etycznych” [Jacek Trzyński i Karina Daniel].

Jak wynika z wypowiedzi Magdaleny Lewandowskiej, podobną postawę przyjmuje Alior Bank:

„(...) wymogi związane z prawem bankowym, które oczekuje od nas pełnej interpretowalności, wyjaśnialności uzyskiwanych rezultatów w procesach kredytowych. W związku z powyższym, rozwiązania typu black box, które mogą być widziane jako sztuczna inteligencja, stosowane są zazwyczaj w obszarach, które nie podlegają tak ścisłej regulacji jak ryzyko kredytowe. Czyli są to obszary związane z CRM’em, hiperpersonalizacją kampanii marketingowych” [Magdalena Lewandowska].

„Powiem o zagrożeniach z mojej perspektywy, szanse oczywiście są ogromne (...) optymalizacje procesowe, działanie szybciej, sprawniej, nowocześniej. Natomiast, co do zagrożeń też jest ich cały szereg. Przede wszystkim bezpieczeństwo danych, bezpieczeństwo IT, kwestie dyskryminacji, brak pełnej kontroli nad algorytmami, szczególnie dostarczonych przez firmy zewnętrzne. (...) Duże modele językowe raczej będą dostarczane przez dostawców zewnętrznych i brak kontroli nad nimi może być sporym wyzwaniem. Też brak interpretowalności no i ostateczna i najważniejsza kwestia – odpowiedzialność za rezultaty generowane przez sztuczną inteligencję. Jednym z use case, które są np. proponowane przez dostawców takich modeli jest chociażby analiza dokumentów bądź regulacji. Moje wieloletnie doświadczenie mówi, że gdy wdrażamy postanowienia jakiejś regulacji, to na końcu jesteśmy odpowiedzialni za zrozumienie i implementację każdego pojedynczego paragrafu, za jego analizę pod kątem ewentualnych luk i zaadresowanie tychże. Rezultaty analizy regulacji przez sztuczną inteligencję mogą być tylko drogowskazem, ale nie są wiążące z perspektywy regulatora, który weryfikuje pełne i kompletne wdrożenie przez bank regulacji” [Magdalena Lewandowska].



Respondenci podkreślali, że **jednym z najpoważniejszych wyzwań towarzyszących prawodawcy dążącemu do uregulowania sztucznej inteligencji, będzie już samo jej legalne zdefiniowanie**, ponieważ – jak ujęła to Magdalena Lewandowska – „definicja AI’a ciągle jest definicją pływającą”. Łukasz Samborski dodaje, że:

„To jest trudne pytanie, bo (...) tych zastosowań jest bardzo dużo różnych. Takich, które wpływają na obsługę klienta i takich, które usprawniają procesy wewnętrzne albo np. zarządzanie strategiczne ryzykiem. Ja się zajmuję tą optymalizacją, do tej pory głównie optymalizacją procesów, więc z mojej działki – olbrzymią zaletą AI i podobnych technologii, często prostszych jest to, że już nam zrewolucjonizowały i jeszcze bardziej zrewolucjonizują codzienną pracę. Mam na myśli pracę banku, wewnętrzne procesy, że będzie szybciej, że będzie taniej, że będzie w wyższej jakości” [Łukasz Samborski].

Biorąc pod uwagę większość wypowiedzi, **ograniczonym entuzjazmem cieszy się koncepcja samoregulacji sektora bankowego w zakresie AI**. Zaryzykować można wręcz tezę, że **reprezentanci sektora bankowego – mający świadomość ryzyk związanych ze sztuczną inteligencją oraz przyzwyczajeni do „twardych” wymogów, wynikających z prawa powszechnie obowiązującego – preferują raczej konkretne i precyzyjne ramy ustawowe niż normy mające oparcie w kodeksach etyki, dobrych praktyk, czy ogólnych wytycznych**, choć dostrzegają również pozytywne strony tej drugiej:

„(...) lepsza samoregulacja niż nic. Jeżeli samoregulacja miałaby być jakimś wstępem do uregulowania tego w sposób taki już sztywny, implementacji na poziomie Polski itd., no bo to też te akty europejskie niezależnie od tego, czy to będzie dyrektywa czy rozporządzenie, mimo że to drugie jest stosowane bezpośrednio, to też generuje jakąś falę zmian w istniejącej legislacji, więc zanim taka fala nastąpi, to pewnie samoregulacja jest wskazana” [Krzysztof Semczuk].

„(...) sam jestem w kilku grupach takich międzybankowych i też widzę, że Związek Banków Polskich stworzył taką grupę pierwszą dotyczącą cyberbezpieczeństwa. Wydaje mi się, że te grupy będą powstawać, one będą miały na razie charakter takiej współpracy między bankami, żeby zastanowić się jak tak naprawdę sprostać tym wyzwaniom, ale finalnie przełoży się to na wydanie

spójnych regulacji, na drodze jakichś częściowo wspólnych procedur, więc moim zdaniem tak, na pewno czekamy na ten AI Act. To będzie coś co wiadomo, że będzie w takiej formie i obowiązować od tego dnia. Natomiast, na pewno później będzie ważne to jak nasze państwo do tego podejdzie i prawdopodobnie zostaną wydane częściowe regulacje, które będą zawsze miały jakąś tam formę dowolności, do której będziemy się dostosowywać i uważam, że to jest jedyna droga tak naprawdę. Muszą być te ramy, bardzo dobrze, że te przepisy powstają. One mają także na celu pokazanie ludziom, że tej technologii można ufać, bo ona w pewien sposób jest też pod nadzorem. No bo to jest główny problem – zaufanie do technologii” [Dawid Kin].

„Na pewno jakiś code of conduct by się naprawdę przydał. Choćby wypracowanie standardów w podejściu do bezpieczeństwa, również po to by biznesowo nie odjechać od rynku. By nie popaść w nadmierny konserwatyzm, bo to po prostu pozbawi nas konkurencyjności” [Magdalena Lewandowska].

„W obliczu postępu technologicznego i rosnącego wykorzystania sztucznej inteligencji na pewno warto rozważyć wszelkie kroki zmierzające do zwiększania cyberbezpieczeństwa, szczególnie w zakresie wykrywania zagrożeń oraz zapewnienia prywatności danych. Innym ważnym obszarem działania jest odpowiedzialność etyczna i prawna. Potrzebne są odpowiednie akty prawne regulujące wykorzystanie AI oraz opracowanie kodeksu zasad etycznych zapewniających uczciwe i transparentne traktowanie klientów (i to nie tylko w sektorze finansowym). Każda instytucja finansowa już teraz, w oparciu o istniejące przepisy, rozporządzenia (w tym unijne AI Act) powinna pracować nad przygotowaniem polityki regulującej najważniejsze kwestie związane z wykorzystaniem technologii AI. Zarządzenia powinny dotyczyć także zasad podziału odpowiedzialności za działania podjęte w oparciu o AI w obszarach: dostawca (jako producent, integrator rozwiązania), bank (jako instytucja decydująca się na wykorzystanie danego rozwiązania), pracownik banku (jako użytkownik systemu podejmujący swoje działania m.in. na podstawie pracy z rozwiązaniem). Oznaczać to będzie pojawienie się m.in. w bankach nowych ról oraz procesów, których celem będzie koordynowanie realizacji powstałych zapisów pod kątem bezpieczeństwa, ochrony danych, minimalizacji ryzyka i zachowania norm etycznych” [Jacek Trzyński i Karina Daniel].

Co ciekawe, respondenci niejednokrotnie dzielili się swoimi przemyśleniami na temat relacji ram regulacyjnych do postępu technologicznego, zaawansowania systemów bankowych oraz nowatorstwa, które pozwala klientom w sposób bardziej efektywny korzystać z oferowanych przez banki produktów. W tym kontekście formułowany był pogląd na temat nowoczesności polskich banków na tle innych krajów Unii Europejskiej, z drugiej strony zaś **obawa przed „przeregulowaniem” nowoczesnych technologii, w tym AI, w prawie unijnym, które – inaczej niż kraje azjatyckie lub USA – niekiedy przesadnie chroni konsumenta usług bankowych, ograniczając w ten sposób postęp technologiczny sektora bankowego:**

„(...) my, jako Polska, jesteśmy bardzo zaawansowani na tle Europy, mamy wiele rozwiązań, które są już bardziej ustabilizowane typu płatności zbliżeniowe. Niekoniecznie wszędzie są takie popularne jak u nas i u nas wydaje się, że wcześniej były już wytestowane i tak samo wydaje mi się w innych przypadkach. Natomiast, ja staram się nie porównywać aż tak do innych kontynentów, gdzie wiem, że te regulacje są trochę bardziej poluzowane” [Dawid Kin].

„(...) jak patrzę w ogóle na obszar Unii Europejskiej, Stanów Zjednoczonych i Azji – to są zupełnie inne obszary, w których jest ciężko ze sobą porównywać, bo tak naprawdę funkcjonujemy w innych uwarunkowaniach prawnych, dochodząc do zupełnie innych konkluzji i dopuszczalnych rozwiązań. W Europie ze szczególną troską podchodzimy do ochrony konsumenta, co w praktyce oznacza, że przedsiębiorcom, zwłaszcza instytucjom finansowym, znacznie mniej wolno. Jak patrzę na rynek azjatycki, konfrontując go z rynkiem unijnym – to są to, wydaje mi się, obszary które trudno w ogóle porównywać ze sobą (...)” [Katarzyna Góra].

„(...) jeśli popatrzymy z takiej perspektywy typowo technologicznej – to myślę, że jesteśmy gdzieś w środku stawki. Jest kilka banków, które działają bardziej dynamicznie, mają rozwiązania na wyższym poziomie, ale też trzeba pamiętać, że one działają w innym otoczeniu regulacyjnym. Tak mówiąc kolokwialnie można im znacznie więcej tak? (...) Uważam, że polskie banki – na tle konkurencji unijnej – cały czas są gdzieś w górnej części stawki jeśli chodzi o adopcję nowych technologii, w tym rozwiązań sztucznej inteligencji” [Rafał Kostowski].

Wypowiedzi większości respondentów wskazują też na to, że **są oni również świadomi faktu, iż AI ACT nie dostarczy odpowiedzi na wszystkie pytania i wątpliwości prawne, otwierając zarazem drogę do dalszych, bardziej szczegółowych regulacji na poziomie krajowym:**

„Wydaje mi się, że jesteśmy na początku tej ścieżki, tzn. główna regulacja czyli AI Act, akt o sztucznej inteligencji, który z grubsza już znamy, ale jak wiadomo jego wdrożenie, data konkretna nie jest znana, ale teraz jak rozumiem właśnie organizują się zarówno banki, jak i inne instytucje finansowe, firmy consultingowe, czyli to właśnie uniwersum instytucji zainteresowanych tematem – komunikuje się i obecnie są tworzone międzybankowe grupy wymiany doświadczeń, także przy firmach consultingowych” [Łukasz Samborski].

2.3. Przykłady rozwiązań inne niż wskazane przez respondentów

Poniżej prezentujemy – niezależne od wskazanych przez respondentów w wywiadach, o których mowa wyżej – przykłady rozwiązań stosowanych dotychczas przez polskie banki, bazujące na technologii sztucznej inteligencji. Omówione projekty i doświadczenia nie wyczerpują oczywiście pełnej gamy zastosowań sztucznej inteligencji w polskim sektorze bankowym, lecz sama ich wielość i różnorodność, pozwala stwierdzić, że **polskie banki są w tym obszarze bardzo aktywne, pełniąc zarazem ważną funkcję prorozwojową oraz edukacyjną (a zatem ogólnospołeczną).**

mBank

mBank w „Strategii Grupy mBanku na lata 2021-2025”⁶ deklaruje planowane rozszerzenie systemu monitoringu oraz reagowania w oparciu o AI.

Bank dąży do stworzenia i wdrożenia co najmniej czterech rozwiązań w bankowości detalicznej i korporacyjnej w oparciu o silniki sztucznej inteligencji AI do 2025 r.:

- 1) zautomatyzowani agenci obsługi klienta,
- 2) wykrywanie nieuczciwych transakcji bankowych,

6 <https://www.mbank.pl/pdf/relacje-inwestorskie/strategia-of-mbank-group-for-2021-2025-pol.pdf>, dostęp: 10 marca 2024 r.



- 3) przewidywanie odejść klientów,
- 4) techniki eksploracji procesów.

Planuje również wykorzystywać AI/ML zarówno do projektowania produktów dla klientów, jak i usprawniania procesów biznesowych.

7

Filary strategii Grupy mBanku na lata 2021-2025

Technologia, bezpieczeństwo i dane jako źródło przewagi



Zapewnimy najwyższe możliwe bezpieczeństwo klientom i pracownikom mBanku poprzez ciągły rozwój wielowarstwowego modelu obrony cyberbezpieczeństwa, zarówno dla rozwiązań lokalnych, jak i chmurowych, obejmujący pełny cykl życia zagrożeń.

Będziemy dążyć do ograniczenia ryzyka materializacji zagrożeń i poprawy skuteczności reagowania:

adekwatne rozwiązania cyberbezpieczeństwa

Działamy proaktywnie, szukając słabych punktów w infrastrukturze mBanku i usuwając podatności, zanim zostaną one wykorzystane. Ponadto, planujemy:

- wzmocnić paradygmat 'security by design' w odniesieniu do regularnych testów kodu tworzonych aplikacji
- ustawicznie kształcić zespół ochrony
- rozszerzyć nasze systemy monitoringu i reagowania o AI/ML

zapobieganie oszustwom i wyłudzeniom

Aby chronić pieniądze naszych klientów, planujemy:

- wdrożyć rozwiązania profilowania klientów w oparciu o dane pozyskane ze źródeł wewnętrznych i zewnętrznych
- wykorzystać sztuczną inteligencję w procesach analizy zachowań klientów
- wykorzystywać biometrię behawioralną w zapobieganiu oszustwom

cele strategiczne

monitorować 80% krytycznych systemów działających w chmurze i przetwarzających dane chronione
testować 80% nowych, krytycznych aplikacji tworzonych w mBanku pod kątem bezpieczeństwa kodu
przeprowadzać co najmniej dwa razy w roku kompleksowe testy zespołu Red Team, weryfikujące poziom bezpieczeństwa organizacji i odporność na pojawiające się cyberzagrożenia
podłączyć 80% procesów wdrażania nowego klienta do systemu zapobiegania oszustwom do 2025 roku

8

Filary strategii Grupy mBanku na lata 2021-2025

Technologia, bezpieczeństwo i dane jako źródło przewagi



Wykorzystamy sztuczną inteligencję i analitykę danych do tworzenia innowacyjnych produktów dla klientów, lepszej oceny ryzyka, zwiększenia efektywności systemów wewnętrznych i przepływu pracy oraz utrzymania wizerunku mBanku jako technologicznego i cyfrowego lidera.

Wykorzystamy technologie AI do wspierania rozwoju oferty mBanku i rozwiązań bezpieczeństwa:

zastosowania sztucznej inteligencji / uczenia maszynowego (AI/ML)

- **zautomatyzowani agenci obsługi klienta** (wykorzystujący technologie analizy głosu i przetwarzania języka naturalnego), pracujący jako osobiści asystenci finansowi w niektórych scenariuszach interakcji (np. w contact center)
- **wykrywanie nieuczciwych transakcji bankowych**, koncentrując się przede wszystkim na operacjach internetowych oraz rozwoju systemów do analizy zachowań klientów w celu ograniczenia ryzyka podszywania się
- **przewidywanie odejść klientów** detalicznych i korporacyjnych, wdrażając algorytmy klasyfikacji oparte na sieciach neuronowych i zwiększając zakres danych
- **techniki eksploracji procesów** dla optymalizacji procesów wewnętrznych

właściwa organizacja

- usprawnić zarządzanie projektami wewnętrznymi z użyciem technologii sztucznej inteligencji
- przyciągnąć więcej specjalistów data science i machine learning
- wykorzystywać AI/ML zarówno do projektowania produktów dla klientów, jak i usprawniania procesów biznesowych

cele strategiczne

stworzyć i wdrożyć co najmniej cztery rozwiązania w bankowości detalicznej i korporacyjnej w oparciu o silniki sztucznej inteligencji (AI) do 2025 roku
wprowadzić co najmniej jeden produkt zorientowany na klienta z wykorzystaniem zewnętrznych systemów uczenia maszynowego w chmurze, dużymi repozytoriami danych i modelami do 2025 roku

7 <https://www.mbank.pl/pdf/relacje-inwestorskie/strategy-of-mbank-group-for-2021-2025-pol.pdf>, dostęp: 10 marca 2024 r.

8 <https://www.mbank.pl/pdf/relacje-inwestorskie/strategy-of-mbank-group-for-2021-2025-pol.pdf>, dostęp: 10 marca 2024 r.

Warto zauważyć, że firma fintechowa z Krakowa, Ailleron, wprowadziła w 2013 r. do mBanku wirtualny oddział LiveBank pod nazwą Ekspert Online. Dzięki temu klienci banku mają możliwość

kontaktu z ekspertami poprzez videokonferencję, nawet za pośrednictwem urządzeń przenośnych, a dodatkowo obsługę klienta wspomaga sztuczna inteligencja⁹.

10



⁹ <https://ailleron.com/pl/case-studies/mbanks-expert-online/>, dostęp: 10 marca 2024 r.

¹⁰ <https://ailleron.com/pl/case-studies/mbanks-expert-online/>, dostęp: 10 marca 2024 r.

„Rosnąca popularność komunikacji za pośrednictwem czatu, a także coraz większe oczekiwania klientów w zakresie transakcji, które mogą wykonać za pomocą tego kanału oraz jak najkrótszego czasu oczekiwania na połączenie z agentem, to wyzwania, przed którymi stoi nie tylko mBank, ale i cały sektor bankowy. Dlatego w 2017 r. zespół Data Scientist mBanku rozpoczął prace nad rozwojem inteligentnego asystenta, którego zadaniem jest wspieranie agentów podczas rozmów z klientami na czacie. Efektem jest mAI ACT, sztuczna inteligencja, która stwarza potencjał do sprostania tym wyzwaniom poprzez automatyzację obsługi części interakcji z klientami. Dzięki współpracy z Ailleron, nowe rozwiązanie zostało z sukcesem wdrożone w 2018 r. w Contact Center mBanku”¹¹.

mBank zorganizował również II edycję programu rozwojowego „Misja innowacja”. W tej edycji bank postawił nacisk na obszar sztucznej inteligencji¹².

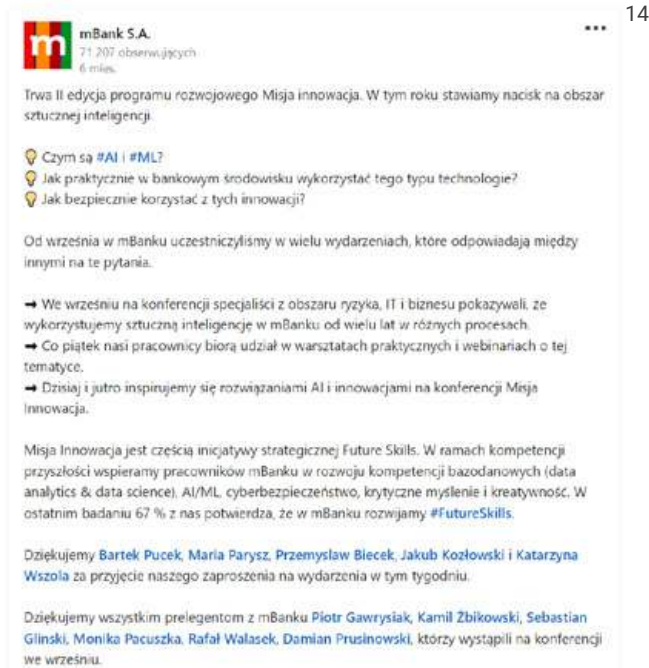
„Całość wydarzenia składała się z dwóch konferencji i konkursu, poprzedzonych cotygodniowymi webinarium i warsztatami z obszaru AI. W ramach konkursu drużynowego interdyscyplinarne zespoły pracowały przez dwa tygodnie nad rozwojem swoich inicjatyw w dwóch kategoriach: projekt wewnętrzny i projekt zewnętrzny. Finałowym zadaniem konkursowym było przedstawienie pomysłu w pięciominutowej prezentacji, na podstawie której jury wyłoniło zwycięzców. 20 wyróżniających się osób zostało nagrodzonych udziałem w wyjeździe edukacyjnym na Florydę – do siedziby NASA

¹¹ <https://livebank24.com/case-studies/mbanks-expert-online/>, dostęp: 10 marca 2024 r.

¹² https://www.linkedin.com/posts/mbank-s-a-ai-ml-futureskills-activity-7130858479241584640-v-7-?utm_source=share&utm_medium=member_desktop, dostęp: 10 marca 2024 r.

i start-upu z branży AI. Misja Innowacja została doceniona przez uczestników – 90% z nich zadeklarowało, że poleciłoby udział w wydarzeniu swoim koleżankom i kolegom”¹³.

Wydarzenie było relacjonowane i promowane za pośrednictwem social mediów banku.



PKO Bank Polski

Jak informuje bank na swojej stronie internetowej: pracowników i użytkowników PKO Banku Polskiego wspiera na wysokim poziomie sztuczna inteligencja¹⁵, co pozwala m.in.:

- ▶ ułatwić klientom korzystanie z usług bankowych;
- ▶ automatyzować coraz więcej procesów wewnętrznych;
- ▶ zapewnić klientom sprawny i niezawodny dostęp do informacji oraz usług, m.in. za pomocą voicebotów.

„Sztuczna inteligencja znajduje coraz szersze zastosowanie w PKO Banku Polskim. Wykorzystywana jest, m.in. w obsłudze klienta i procesach wewnętrznych, a także coraz szerzej w ocenie ryzyka i na potrzeby CRM. AI ułatwia klientom korzystanie z usług bankowych i umożliwia przygotowanie dla nich najlepszej oferty. Pracowników banku wspiera w codziennej pracy, wykonując za nich proste i najbardziej czasochłonne czynności. Wpływa na poprawę efektywności i zwiększa bezpieczeństwo w różnych obszarach funkcjonowania banku. (...). Najbardziej znane rozwiązania AI w PKO Banku Polskim to voiceboty, a wśród nich Asystent głosowy w aplikacji IKO, który pomaga klientom korzystać z usług bankowych. Można do niego mówić lub pisać językiem naturalnym, czyli tak, jak robimy to z ludźmi. Potrafi, m.in. zrobić przelew, podać kod BLIK, zmienić limit na karcie lub ją zastrzec. Gdy klient zapyta o swoje wydatki, Asystent pomoże je przeanalizować w formie przejrzystych wykresów, a gdy chce wymienić walutę skieruje do kantoru. Obecnie rozumie już ponad 320 tematów rozmów i skorzystał z niego już milion klientów banku”¹⁶.

PKO Bank Polski popularyzuje również wiedzę na temat stosowanych przez siebie rozwiązań, wykorzystujących sztuczną inteligencję, na portalach społecznościowych¹⁷.

„**#SztucznaInteligencja** jest motorem zmiany. I dla nas staje się ważnym narzędziem, które pozwoli spojrzeć inaczej na potrzeby klientów i dostarczać spersonalizowane produkty.”

Dyrektor Pionu Rozwoju i Utrzymania Aplikacji w PKO Banku Polskim zapewnia, że **sztuczna inteligencja staje się kluczowym narzędziem umożliwiającym wprowadzenie hiperpersonalizacji**, co pozwala na nowo definiować potrzeby klientów. Oznacza to nie tylko dostosowanie oferty do indywidualnego odbiorcy, ale również uwzględnienie najlepszego czasu, miejsca i kontekstu dla danej osoby. Obecnie oferta PKO Banku Polskiego dla klientów korporacyjnych jest wysoko spersonalizowana, bank planuje

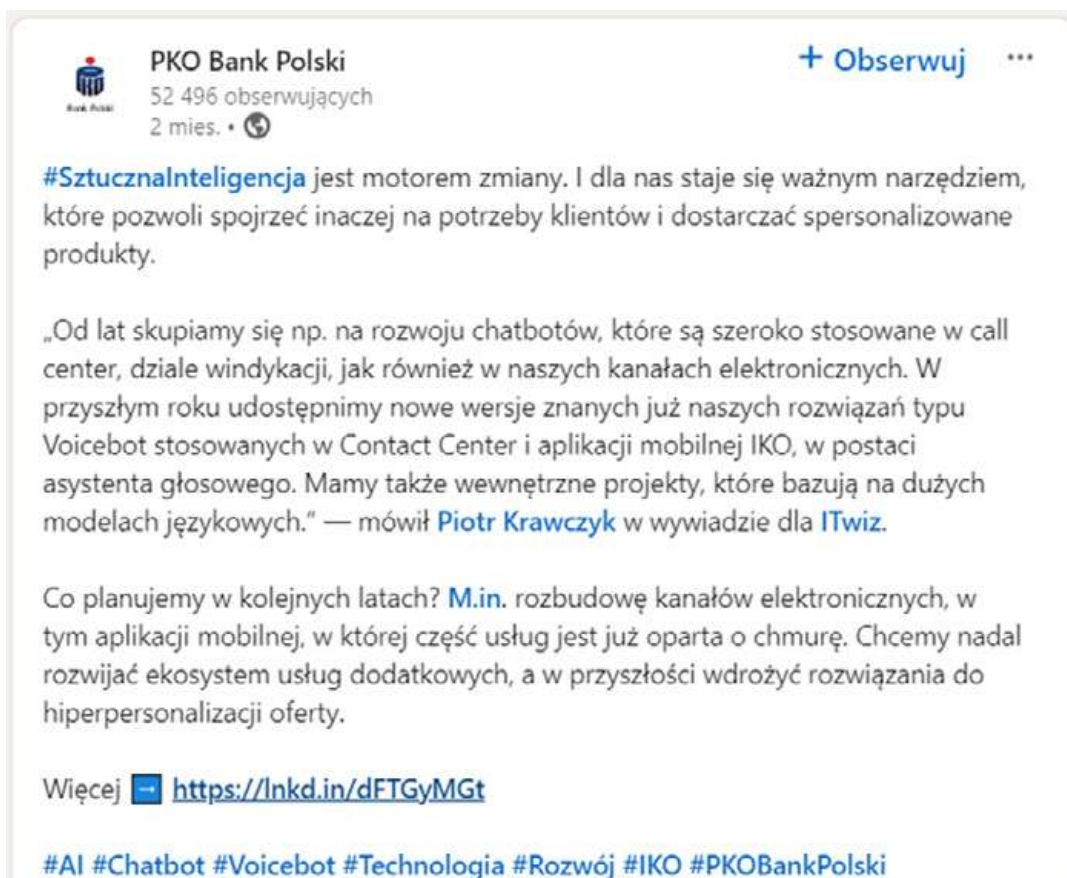
13 <https://www.pb.pl/wsparcie-rozwoju-pracownikow-nowe-kompetencje-w-nowej-rzeczywistosci-nagroda-glowna-mbank-1209188#:~:text=W%202023%20r.,i%20warsztatami%20z%20obszaru%20AI>, dostęp: 10 marca 2024 r.

14 <https://www.linkedin.com/posts/mbank-s-a-ai-ml-futureskills-activity-7130858479241584640-v-7?originalSubdomain=pl>, dostęp: 10 marca 2024 r.

15 <https://media.pkobp.pl/235842-sztuczna-inteligencja-wspiera-klientow-i-pracownikow-pko-banku-polskiego>, dostęp: 10 marca 2024 r.

16 <https://media.pkobp.pl/235842-sztuczna-inteligencja-wspiera-klientow-i-pracownikow-pko-banku-polskiego>, dostęp: 10 marca 2024 r.

17 https://www.linkedin.com/posts/pko-bp-sztuczna-inteligencja-ai-chatbot-activity-7148304552084103168-Fau4?utm_source=share&utm_medium=member_desktop, dostęp: 10 marca 2024 r.



udostępnić podobną personalizację także klientom indywidualnym.

Oprócz hiperpersonalizacji bank realizuje wiele innych projektów z zakresu AI, w tym **rozwój chatbotów** używanych w różnych działach oraz wprowadzenie **nowych wersji voicebotów** w Contact Center i aplikacji mobilnej. Bank pracuje także nad wewnętrznymi projektami wykorzystującymi duże modele językowe, takie jak „PKO Prosto”, które mają na celu upraszczanie komunikacji z klientami, eliminując branżowy żargon.

W jednym z wywiadów Dyrektor Piotr Krawczyk przekonuje:

„Docelowo IKO ma być tzw. superaplikacją. Aby jednak jej użytkownik nie „pogubił się” w tej ofercie, konieczna jest hiperpersonalizacja i wykorzystanie AI. To sztuczna inteligencja poprowadzi klientów po szerokiej ofercie usług udostępnianych przez PKO Bank Polski. (...) Rozpoczynamy projekty AI skupiające się na obszarze IT, przede wszystkim związane z automatyzacją testów. Narzędzia bazujące na algorytmach AI będzie-

my wykorzystywać też w obszarze CyberSecurity. Wszystkie te projekty są elementem naszej strategii AI@Scale”¹⁹.

Kluczem do optymalnego wykorzystania nowoczesnych technologii, w tym zapewnienia jej efektywności oraz zarazem bezpieczeństwa, jest **permanentne wzmacnianie działów IT nowymi pracownikami, szczególnie analitykami, architektami, kierownikami projektów i programistami, a także ekspertami od hurtowni danych, administratorami aplikacji lub inżynierami**. W konsekwencji PKO BP prezentowane jest **nie tylko jako typowy bank, lecz jednocześnie potężna firma technologiczna**:

„Prowadzimy równocześnie wiele projektów informatycznych, które są bardzo złożone i które

18 https://www.linkedin.com/posts/pko-bp_newsletter-sztucznainteligencja-ai-activity-7090941518806454272-clBH?originalSubdomain=pl, dostęp: 10 marca 2024 r.

19 A. Jadcak, AI poprowadzi klientów po szerokiej ofercie naszych usług. Wywiad z P. Krawczykiem, <https://itwiz.pl/ai-poprowadzi-klientow-po-szerokiej-ofercie-naszycz-uslug/>, dostęp: 10 marca 2024 r.

ze względu na skalę naszej działalności, mają duży wpływ na rynek. Jesteśmy olbrzymią firmą technologiczną, ale jednocześnie jako największy bank w Polsce mamy bardzo solidne fundamenty, co stwarza unikalne środowisko pracy. Dzięki temu naszym pracownikom możemy zapewnić nie tylko ciekawą ścieżkę rozwoju, ale i stabilność zatrudnienia”²⁰.

Inne przykłady wykorzystania AI w PKO Banku Polskim:

- ▶ „Talk to IKO” – asystent głosowy dostępny w aplikacji mobilnej IKO (umożliwia wykonanie najbardziej popularnych operacji bankowych, jak przelew, przelew na telefon, doładowanie telefonu, wyświetlenie kodu Blik, przeszukanie historii, podanie salda i wiele innych);
- ▶ Emplot – inteligentny chatbot rekrutacyjny umożliwiający kandydatom do pracy w banku rozmowę, na podstawie której bot dokonuje wstępnej, automatycznej selekcji aplikacji, zgodnie z preferencjami kandydatów, dopasowując ich aplikacje do odpowiedniej ścieżki rekrutacyjnej (dostępny 24 godziny na dobę i pozwala na prowadzenie kilku rozmów jednocześnie);
- ▶ Voiceboty obsługowe – boty głosowe umożliwiające telefoniczną obsługę klientów, dotyczącą m.in. nawigacji na infolinii, ankiet satysfakcji klienta czy zaległych spłat produktów kredytowych;
- ▶ Koronabot – specjalnie wdrożony na infolinię voicebot, który pomagał klientom, odpowiadając na pytania dotyczące działalności banku w trakcie pierwszej fali pandemii koronawirusa;
- ▶ Wideoweryfikacja – narzędzie, które umożliwia zakładanie przez klientów konta za pomocą „selfie” dzięki funkcjom inteligentnego rozpoznawania obrazu i biometrii²¹.

Bank Pekao S.A.

Bank Pekao S.A. zapewnia, że – dzięki wykorzystaniu najnowocześniejszych narzędzi z zakresu automatyzacji, w tym wykorzystaniu technologii sztucznej inteligencji – dostarcza jeszcze sprawniejszej i szybszej obsługi za pośrednictwem internetowego systemu PekaoBiznes²⁴.

„Bank Pekao S.A. konsekwentnie podąża w kierunku digitalizacji obsługi klientów biznesowych. Wprowadzona nowość to połączenie funkcjonalności systemu bankowości elektronicznej PekaoBiznes24 z optycznym rozpoznawaniem znaków (ang. Optical Character Recognition, OCR), uczeniem maszynowym i automatyzacją procesów. Dzięki temu bank jest w stanie dużo szybciej niż do tej pory interpretować i kategoryzować zdalnie przekazane przez klienta dokumenty, niezależnie od ich formy.

Zastosowane przez bank rozwiązania to tzw. hiperautomatyzacja, czyli połączenie sztucznej inteligencji (ang. Artificial Intelligence, AI), uczenia maszynowego (ang. Machine Learning, ML) i zrobotyzowanej automatyzacji procesów (ang. Robotic Process Automation, RPA). Hiperautomatyzacja pomaga usprawnić zachodzące w banku procesy biznesowe i przetworzyć posiadane dane w sposób nieosiągalny dla tradycyjnych metod”²².

Bank poinformował publicznie o rozpoczęciu współpracy strategicznej, obejmującej m.in. wykorzystanie sztucznej inteligencji, z firmą Synerise S.A.²³. Kooperacja ta obejmować ma m.in. **projekty edukacji uczniów i nauczycieli oraz wsparcie cyfryzacji małych i średnich przedsiębiorstw**.

„Strategiczne partnerstwo Banku Pekao z firmą Synerise, która stworzyła innowacyjną platformę zaawansowanych usług analitycznych opartych na sztucznej inteligencji (AI), ma na celu rozwój cyfryzacji społeczeństwa. Proces ten jest możliwy dzięki edukacji oraz udostępnianiu najnowocześniejszych technologii i rozwiązań analitycznych służących bankowi, a także jego klientom.

20 <https://media.pkobp.pl/261850-pko-bank-polski-rozbudowuje-zespoly-it>, dostęp: 10 marca 2024 r.

21 You & AI – sztuczna inteligencja w Banku Przyszłości, <https://www.karierawfinansach.pl/przewodnik/2020/projekty/you-and-ai#menu-1>, dostęp: 10 marca 2024 r.

22 <https://media.pekao.com.pl/pr/799931/bank-pekao-s-a-wprowadza-hyperautomatyzacje-obslugi-klienta-biznesowego-będzie-latwiej-szybciej-nowocześniej>, dostęp: 10 marca 2024 r.

23 <https://media.pekao.com.pl/pr/419112/bank-pekao-z-synerise-ida-w-strone-sztucznej-inteligencji>, dostęp: 10 marca 2024 r.

Bank Pekao S.A. wprowadza hiperautomatyzację obsługi klienta biznesowego – będzie łatwiej, szybciej, nowocześniej

[← Powrót](#)

Małe i Średnie Firmy 4.04.2023

Dzięki wykorzystaniu najnowocześniejszych narzędzi z zakresu automatyzacji, sztucznej inteligencji oraz zaawansowanej analityki, Bank Pekao S.A. zapewni klientom biznesowym jeszcze sprawniejszą i szybszą obsługę za pośrednictwem systemu PekaoBiznes24.

Bank Pekao S.A. konsekwentnie podąża w kierunku digitalizacji obsługi klientów biznesowych. Wprowadzona nowość to połączenie funkcjonalności systemu bankowości elektronicznej PekaoBiznes24 z optycznym rozpoznawaniem znaków (ang. Optical Character Recognition, OCR), uczeniem maszynowym i automatyzacją procesów. Dzięki temu bank jest w stanie dużo szybciej niż do tej pory interpretować i kategoryzować zdalnie przekazane przez klienta dokumenty, niezależnie od ich formy.

Zastosowane przez bank rozwiązania to tzw. hiperautomatyzacja, czyli połączenie sztucznej inteligencji (ang. Artificial Intelligence, AI), uczenia maszynowego (ang. Machine Learning, ML) i zrobotyzowanej automatyzacji procesów (ang. Robotic Process Automation, RPA). Hiperautomatyzacja pomaga usprawnić zachodzące w banku procesy biznesowe i przetworzyć posiadane dane w sposób nieosiągalny dla tradycyjnych metod.

– Hiperautomatyzacja przenosi transformację cyfrową i jakość oraz tempo obsługi klienta na kolejny, wyższy poziom. W uproszczeniu można powiedzieć, że „nakarmiliśmy” algorytm skanami dokumentów naszych klientów, dzięki czemu nauczył się on ich rozpoznawania. Gdy algorytm otrzymuje kolejny plik, to po jego przeanalizowaniu jest w stanie dokładnie określić, z jakim dokumentem ma do czynienia. Nie jest istotne, czy klient korzystał ze wzoru, czy samodzielnie napisał dyspozycję. Co więcej, algorytm potrafi „wyluskać” z otrzymanego dokumentu kluczowe dla nas informacje, potrzebne do dalszego, sprawnego procesowania – tłumaczy Jędrzej Fryc z Departamentu Bankowości Elektronicznej i Digitalizacji Procesów – pomysłodawca wdrożenia tego rozwiązania dla klientów firmowych w Banku Pekao S.A.

Proponowane Informacje

Małe i Średnie Firmy

Bank Pekao wprowadza Kredyt Unia - nowe rozwiązanie dla beneficjentów dotacji unijnych, w tym środków pochodzących z KPO

16.04.2024

[Przejdź](#)

Microsoft zapewnia potrzebne do realizacji programu zaplecze technologiczne.

Pierwszym obszarem rozpoczętej współpracy jest AI Schools & Academy, program kształcenia dzieci i młodzieży z zakresu sztucznej inte-

ligencji. Ma on inicjować projekty edukacyjne budujące cyfrową świadomość i kompetencje wśród uczniów oraz ich nauczycieli. W ramach programu sfinansowane zostaną zajęcia dodatkowe w 1500 szkołach i przedszkolach. Pozwolą uczniom rozwijać swoje umiejętności, poszerzać

Bank Pekao z Synerise idą w stronę sztucznej inteligencji

[← Powrót](#)

Małe i Średnie Firmy 24.01.2019

Bank Pekao S.A. i Synerise S.A., przy współpracy z Microsoft, rozpoczynają współpracę strategiczną, która obejmie projekty edukacji uczniów i nauczycieli oraz wsparcie cyfryzacji małych i średnich przedsiębiorstw.

Strategiczne partnerstwo Banku Pekao z firmą Synerise, która stworzyła innowacyjną platformę zaawansowanych usług analitycznych opartych o sztuczną inteligencję (AI), ma na celu rozwój cyfryzacji społeczeństwa. Proces ten jest możliwy dzięki edukacji oraz udostępnianiu najnowocześniejszych technologii i rozwiązań analitycznych służących bankowi, a także jego klientom. Microsoft zapewnia potrzebne do realizacji programu zaplecze technologiczne.

Pierwszym obszarem rozpoczętej współpracy jest AI Schools & Academy, program kształcenia dzieci i młodzieży z zakresu sztucznej inteligencji. Ma on inicjować projekty edukacyjne budujące cyfrową świadomość i kompetencje wśród uczniów oraz ich nauczycieli. W ramach programu sfinansowane zostaną zajęcia dodatkowe w 1500 szkołach i przedszkolach. Pozwolą uczniom rozwijać swoje umiejętności, poszerzać zakres zainteresowania nowymi technologiami, a także aktywizować kadrę nauczycielską do rozwoju swoich kompetencji.

Rolą banku w programie będzie stworzenie uczestnikom możliwości wykorzystania w praktyce nabytych umiejętności poprzez udział w konkursach, hackathonach oraz stażach.

Proponowane Informacje

Małe i Średnie Firmy

Bank Pekao wprowadza Kredyt Unia - nowe rozwiązanie dla beneficjentów dotacji unijnych, w tym środków

24

24 <https://media.pekao.com.pl/pr/419112/bank-pekao-z-synerise-ida-w-strone-sztucznej-inteligencji#:~:text=Pierwszym%20obszarem%20rozpocz%C4%99tej%20wsp%C3%B3lpracy%20jest,w%C5%9Br%C3%B3d%20uczni%C3%B3w%20oraz%20ich%20nauczycieli>, dostęp: 10 marca 2024 r.



zakres zainteresowania nowymi technologiami, a także aktywizować kadrę nauczycielską do rozwoju swoich kompetencji²⁵.

Ponadto bank **dzieli się na swoich social mediach treściami dotyczącymi sztucznej inteligencji oraz nowoczesnych technologii, promując wiedzę o nich**²⁶.

Santander Bank Polska

W sprawozdaniu finansowym za 2023 r. Prezes Zarządu Santander Bank Polska Michał Gajewski informował o rozwoju sztucznej inteligencji i postępach w cyfryzacji spółki²⁸.

„W ubiegłym roku byliśmy świadkami dynamicznego rozwoju sztucznej inteligencji. Zdajemy sobie sprawę, że sztuczna inteligencja

25 <https://media.pekao.com.pl/pr/419112/bank-pekao-z-synerise-ida-w-strone-sztucznej-inteligencji#:~:text=Pierwszym%20obszarem%20rozpocz%C4%99tej%20wsp%C3%B3lnej%20pracy%20jest,w%C5%9Br%C3%B3d%20uczni%C3%B3w%20oraz%20ich%20nauczycieli>, dostęp: 10 marca 2024 r.

26 https://www.linkedin.com/posts/bank-pekaosa_pekao-ai-activity-7142882511449223168-Rbmg?utm_source=share&utm_medium=member_desktop, dostęp: 10 marca 2024 r.

27 https://www.linkedin.com/posts/bank-pekaosa_pekao-ai-activity-7142882511449223168-Rbmg?originalSubdomain=pl, dostęp: 10 marca 2024 r.

28 https://www.santander.pl/regulation_file_server/time20240216092649/download?id=166863&lang=en_US, dostęp: 10 marca 2024 r.



Dear All,

the year of 2023 was a fruitful time for Santander Bank Polska Group. We had many successes in various areas of our business.

We focused on achieving our goals – improvement of customer experience, digitalisation and responsible banking. We have proved that our purpose of helping people and businesses prosper is reflected both in the social and financial dimension. High NPS for customer experience and our solid financial results confirm that our initiatives in these areas have been effective.

Santander Bank Polska Group closed 2023 with attributable profit of PLN 4.8bn. Our sales volumes grew noticeably. Income increased by 29% YoY to PLN 16bn. Customer deposits and gross loan portfolio grew 7% and 4% YoY, respectively. We have a sound capital position and our liquidity ratios comfortably above the required levels.

We have been developing our product offer by introducing solutions that are useful to our customers. One of our priorities is to ensure that our customers' funds and personal data are secure – that is why we continue to invest in cybersecurity solutions.

Several trends dominated the economy in 2023. We witnessed faster-than-expected disinflation coupled with the rebound of the GDP growth. Investments grew fast while consumption remained low. Foreign trade turnover was in a clear downward trend. The global economy continued its soft landing. In general, however, it was a good year for the banking sector. The financial condition of households and companies remained stable, hence the cost of risk did not increase. Interest rates remained quite high, despite a 1 p.p. cut before the parliamentary elections. The demand for loans started to revive, primarily in the home mortgage segment – thanks to the First Apartment programme – as well as in the consumer finance segment.

Last year we witnessed a rapid development of AI. We are aware AI may revolutionise the business, interactions with customers and our everyday work. We are conscious of the challenges it takes to use AI responsibly. We actively apply advanced technologies, such as cloud computing and Big Data. They help us better understand and respond to customers' needs, and improve business processes.

We keep monitoring market environment so as to anticipate expectations and trends. This is why we have embarked on our new strategy for 2024–2026 **"We Help You Achieve More"**. Its three key pillars are: Total Experience, Total Digitalisation and Total Responsibility. We believe that building the best experience and evoking positive emotions should accompany our relations with customers and employees. They are at the heart of everything we do. We want to deliver the highest returns for our shareholders, have outstanding results and achieve our ambition of being the most profitable bank in Poland. We will do it responsibly, taking care of sustainable growth and proper management of operational risk. These aspects are related to our environmental, social and governance commitments. We also put effort in responsible digital transformation, sustainable financing, educational initiatives addressed to different segments of society, mitigating climate change and reducing our environmental footprint. Whatever we do for our customers, employees or shareholders, we want to do it in a responsible manner and in line with top ethical standards.

Individuals and companies who use our products and services appreciate our focus on customer needs.

In the retail segment, we implemented a modern mobile application. Thanks to the intuitive migration process, more than 2.5m users migrated to the new app during one month. We continued to simplify and digitise our products and processes. This was coupled with the development of new multi-channel processes and top-level customer service in remote channels.

*może zrewolucjonizować biznes, interakcje z klientami i codzienną pracę. Zdajemy sobie sprawę z wyzwań związanych z odpowiedzialnym korzystaniem ze sztucznej inteligencji i zaawansowanych technologii. Aktywnie stosujemy zaawansowane technologie, takie jak przetwarzanie w chmurze i Big Data. Pomagają nam one lepiej rozumieć potrzeby klientów i reagować na nie, a także usprawniać procesy biznesowe*²⁹.

Santander Consumer Bank

Santander Consumer Bank przeprowadził **kampanię marketingową zatytułowaną „Komunikacja stworzona z AI”, promującą sztuczną inteligencję oraz jej możliwości**. Stworzone teksty i obrazy kampanii zostały stworzone za pomocą AI.

„Nasze działania były pionierskie, ponieważ – według naszej wiedzy – żaden inny bank nie podjął się wyzwania jednoczesnego generowania treści i obrazów reklamowych przy użyciu AI.

Mieliśmy dwie koncepcje, po pierwsze, chcieliśmy pokazać, że to, co tworzy AI może stać się

29 https://www.santander.pl/regulation_file_server/time20240216092649/download?id=166863&lang=en_US, dostęp: 10 marca 2024 r.

Rozpoczęliśmy kampanię marketingową „Komunikacja stworzona z AI” ³¹



rzeczywistością dzięki kredytom Santander Consumer Banku. Po drugie, zależało nam, żeby w przekazie uczłowieczyć sztuczną inteligencję, podkreślić że jest wszędzie i nigdy nie zasypia, podobnie jak nasze procesy, dzięki którym klienci mogą skorzystać z finansowania 24h/7.

Dla zadowalających efektów bardzo ważne było tworzenie odpowiednich zapytań. Następnie, po obserwacji pierwszych wyników, nasz bank pogłębiał dialog ze sztuczną inteligencją, zasilał ją kolejnymi danymi. Metodą prób i błędów udało się odwzorować przyjęte założenia, czego efekty można oglądać m.in. na stronie internetowej Santander Consumer Banku³⁰.

ING Bank Śląski

ING Bank Śląski przeprowadził m.in. akcję „Ja w przyszłości. Powered by AI & ING”³², zachęcając Polaków do rozważania swojej przyszłości finanso-

wej i życia na emeryturze. W tym celu wykorzystał technologię kreowania obrazów przez sztuczną inteligencję.

„Tam gdzie zawodzi ludzki umysł z pomocą przychodzi... sztuczna inteligencja. ING w akcji „Ja w przyszłości. Powered by AI & ING”, wykorzystał technologię do stworzenia obrazów jutra, to znaczy ludzi na emeryturze widzianych oczami AI. Wystarczy wgrać zdjęcie i odpowiedzieć na pytanie: „Co chcesz robić w przyszłości”. Relaks w wertykalnych ogrodach miasta przyszłości? A może lot komercyjny na Księżyc? Tu wszystko może się zdarzyć. Codziennie 21 najciekawszych pomysłów zamieni się w cyfrowe obrazy.

Większość elementów promujących akcję „Ja w przyszłości. Powered by AI & ING” także zostało przygotowanych w oparciu o sztuczną inteligencję. Zarówno wygenerowane wideo, jak i głos oraz muzyka zostały stworzone przez algorytmy sztucznej inteligencji, a rolę człowieka było tylko określenie głównego przekazu i złożenie tego co powstało w całość. W efekcie powstała wizualizacja przyszłości opowiedziana „oczami” AI³³.

³⁰ <https://www.blog.santanderconsumer.pl/bank-mozliwosci/rozpoczelismy-kampanie-marketingowa-komunikacja-stworzona-z-ai,1,247.html>, dostęp: 10 marca 2024 r.

³¹ <https://www.blog.santanderconsumer.pl/bank-mozliwosci/rozpoczelismy-kampanie-marketingowa-komunikacja-stworzona-z-ai,1,247.html>, dostęp: 10 marca 2024 r.

³² <https://www.ja-w-przyszlosci.pl/>, dostęp: 10 marca 2024 r.

³³ <https://www.wirtualnemedi.pl/arttykul/ing-bank-slaski-sztuczna-inteligencja>, dostęp: 10 marca 2024 r.

ING zwizualizuje Twoją wizję przyszłości dzięki AI ³⁴

09 stycznia 2023 | Akcje marketingowe i promocje | ING BANK ŚLĄSKI S.A.



ING pokazuje przyszłość polskich miast za pomocą AI ³⁶

12 stycznia 2023 | Akcje marketingowe i promocje | ING BANK ŚLĄSKI S.A.



ING Bank Śląski pragnie zainspirować Polaków do refleksji i dyskusji na temat ich przyszłości finansowej i życia na emeryturze. Aby to osiągnąć, posłużył się technologią – algorytmami tworzenia obrazów przez Sztuczną Inteligencję (AI). W ramach akcji „Ja w przyszłości. Powered by AI & ING” bank podejmuje wyzwanie wizualizacji przyszłości polskich metropolii, jak również poszczególnych internautów. Wizja siebie i dobrze nam znanych miejsc w przyszłości ma zachęcić do myślenia o tym, co czeka nas za kilkanaście czy kilkadziesiąt lat i zadbania o tą przyszłość już teraz.

Jak tłumaczyła Barbara Pasterczyk, Dyrektor Banku odpowiedzialna za komunikację marketingową:

„O życiu na emeryturze nie myślimy często, a ponad 20% młodych ludzi nie myśli o nim w ogóle. Blisko połowa badanych Polaków nie rozmawiała z nikim przez ostatnie 6 miesięcy na ten temat. Ci, którym się to zdarza przyznają, że są to raczej pesymistyczne skojarzenia związane z lękiem (42%), a nie z nadzieją (23%). Chcemy oswajać Polaków z myślą o ich przyszłości finansowej a także zachęcić

ich do rozmawiania o emeryturze i wizualizowania jej. Wierzymy, że to zwiększy ich szanse na podjęcie działania i wypracowanie skutecznego, długoterminowego planu. Teraz z pomocą sztucznej inteligencji mogą zobaczyć swoją przyszłość co być może spowoduje, że chętniej podejną do tematu oszczędzania z myślą o przyszłości. Zachęcamy do wzięcia spraw w swoje ręce i podejmowania działań tu i teraz a nie odkładania ich na później”³⁵.

³⁴ <https://media.ing.pl/informacje-prasowe/926/pr/786347/ing-zwizualizuje-twoja-wizje-przyszlosci-dzieki-ai>, dostęp: 10 marca 2024 r.

³⁵ <https://media.ing.pl/informacje-prasowe/926/pr/786347/ing-zwizualizuje-twoja-wizje-przyszlosci-dzieki-ai>, dostęp: 10 marca 2024 r.

³⁶ <https://media.ing.pl/informacje-prasowe/926/pr/786868/ing-pokazuje-przyszlosc-polskich-miast-za-pomoca-ai>, dostęp: 10 marca 2024 r.



37



40

Akcje takie wydają się szczególnie atrakcyjne w kontekście **promocji pożądaných postaw dotyczących nie tylko indywidualnego życia poszczególnych osób (np. oszczędność, planowanie przyszłości, zdrowy tryb życia czy decyzje emerytalne), lecz również ważnych spraw ogólnospołecznych – jak np. zrównoważony rozwój, ekologia, tolerancja, bezpieczeństwo w ruchu drogowym, partycypacja społeczna, empatia.**

Innym przejawem aktywności banku w obszarze nowoczesnych technologii, jest wydarzenie HackING, którego tematem przewodnim są rozwiązania z zakresu AI³⁸.

„Celem HackING jest zbudowanie społeczności skupionej wokół rozwiązań AI oraz przybli-

żenie młodym talentom zagadnień związanych z wykorzystaniem źródeł danych, technologii i narzędzi w instytucjach finansowych. W pierwszej edycji uczestnicy konkursu będą mogli dowiedzieć się jak wygląda praca w IT w banku oraz zapoznać się z nowoczesnymi technikami AI. Przy wsparciu doświadczonych mentorów i ekspertów, będą mieli okazję stworzyć swój własny model rozpoznawania i klasyfikacji dokumentów. Zadanie konkursowe będzie polegało na przygotowaniu modelu rozpoznawania i klasyfikacji dokumentów na podstawie spreparowanych danych w postaci tekstów i skanów”³⁹.

37 <https://www.ja-w-przyszlosci.pl/>, dostęp: 10 marca 2024 r.

38 <https://media.ing.pl/informacje-prasowe/926/pr/804614/pierwsza-edycja-hacking-hackathonu-ing-banku-slaskiego-tematem-przewodnim-wydarzenia-beda-rozwiazania-z-zakresu-ai>, dostęp: 10 marca 2024 r.

39 <https://media.ing.pl/informacje-prasowe/926/pr/804614/pierwsza-edycja-hacking-hackathonu-ing-banku-slaskiego-tematem-przewodnim-wydarzenia-beda-rozwiazania-z-zakresu-ai>, dostęp: 10 marca 2024 r.

40 <https://media.ing.pl/informacje-prasowe/926/pr/804614/pierwsza-edycja-hacking-hackathonu-ing-banku-slaskiego-tematem-przewodnim-wydarzenia-beda-rozwiazania-z-zakresu-ai>, dostęp: 10 marca 2024 r.

42

ING Polska
46 280 obserwujących
1 mies. • Edytowano •

+ Obserwuj ...

- AI to nie tylko technologia i chat GPT. To szeroko zakrojona zmiana, do której musimy dodać swój wkład i budować własne zasoby. Trzeba inwestować w ludzi, w modele i w dane. Musimy mieć przygotowane i świadome społeczeństwa aby w dużej skali i skutecznie wykorzystać zachodzące zmiany. Jestem optymistką jeżeli chodzi o polskie firmy i ich możliwości dostosowania. Sztuczna inteligencja nie jest dla nich celem samym w sobie. Ma pomagać w prowadzeniu biznesu i podnoszeniu efektywności działania. Firmy muszą nauczyć się wychwytywać szanse, które stwarza AI i szybko implementować rozwiązania zwiększające przewagę konkurencyjną. My, tak jak dotychczas, będziemy wspierać firmy w tych działaniach, wykorzystując możliwości jakie daje nam sztuczna inteligencja. Jeżeli chodzi o wyłaniające się trendy i obszary o szerokim zastosowaniu AI przewiduje się, że będą to kwestie bezpieczeństwa, zarówno w zakresie ochrony przed cyber przestępcami jak i ochrony naszych praw i całych systemów demokracji - powiedziała **Ewa Łuniewska**, Wiceprezes Zarządu ING Banku Śląskiego, podczas debaty Cyfrowa gospodarka, cyfrowa firma. Najważniejsze trendy technologiczne roku 2024, na EEC Trends 2024 w Warszawie.

W dyskusji moderowanej przez **Sebastian Ogórek**, kierownika działu gospodarka w Gazecie Wyborczej i szefa redakcji **Wyborcza.biz** uczestniczyli również:

- **Ireneusz Borowski**, Country Manager Poland, **Dassault Systèmes**
- **Radosław Franczak**, partner, Technology Consulting Leader, **EY Polska**
- **Marek Gabryś**, prezes zarządu, współwłaściciel, **AIUT Sp. z o.o.**
- **Dariusz Mazurkiewicz**, prezes zarządu Polskiego Standardu Płatności, operatora **BLIK**

43

ING Polska
46 280 obserwujących
3 mies. •

+ Obserwuj ...

W ING zależy nam na wdrażaniu innowacyjnych rozwiązań – w tym tych opartych o sztuczną inteligencję. Dlatego tworzymy program **#AITrek**, który pomaga nam w budowaniu naszych zdolności wykorzystania nowoczesnych technologii.

Za nami kolejny krok programu – finał, podczas którego zobaczyliśmy prezentacje pomysłów na wykorzystanie sztucznej inteligencji w banku. Wyłoniliśmy spośród nich te najlepsze. Tym samym rozpoczynamy kolejną misję AI Trek'owej podróży i będziemy pracowali nad dalszym rozwojem pomysłów.

ING Bank Śląski działa **na rzecz rozwoju sztucznej inteligencji w bankowości na portalach społecznościowych**⁴¹.

Doniosłość sztucznej inteligencji oraz możliwości, jakie daje, akcentuje Ewa Łuniewska, Wiceprezes Zarządu ING Banku Śląskiego:

„AI to nie tylko technologia i chat GPT. To szeroko zakrojona zmiana, do której musimy dodać swój wkład i budować własne zasoby. Trzeba inwestować w lu-

dzi, w modele i w dane. Musimy mieć przygotowane i świadome społeczeństwa aby w dużej skali i skutecznie wykorzystać zachodzące zmiany.”.

Ponadto ING Bank Śląski stworzył Program **#AITrek**, który ma na celu pomóc w budowaniu zdolności wykorzystania nowoczesnych technologii:

41 https://www.linkedin.com/posts/ingpolska_ai-to-nie-tylko-technologia-i-chat-gpt-activity-7161388866959011840-ytMk/?originalSubdomain=pl, dostęp: 10 marca 2024 r.

42 https://www.linkedin.com/posts/ingpolska_ai-to-nie-tylko-technologia-i-chat-gpt-activity-7161388866959011840-ytMk/?originalSubdomain=pl, dostęp: 10 marca 2024 r.

43 https://www.linkedin.com/posts/ingpolska_aitrek-ing-activity-7137404718854606848-nqUr/?originalSubdomain=pl, dostęp: 10 marca 2024 r.



BNP Paribas

BNP Paribas informuje na swoich stronach internetowych o możliwościach oferowanych przez technologię sztucznej inteligencji, w tym dla klientów banku:

„szczególnie duży potencjał aplikacyjny AI mają trzy obszary sektora finansowego:

- spersonalizowane planowanie finansowe,
- wykrywanie nadużyć i przeciwdziałanie praniu brudnych pieniędzy,
- automatyzacja procesów – zarówno w ramach back office, jak i obsługi klienta. (...)

Już teraz coraz większą rolę na rynku finansowym odgrywa tzw. robo-doradztwo (robo-advisory) – czyli zautomatyzowane usługi inwestycyjne, oparte na algorytmach komputerowych (...) Rozwiązania takie pojawiły się już na rynku polskim, w tym m.in. w działalności banków Santander Bank Polska i ING Bank Śląski oraz BGŻ BNP Paribas. Ten ostatni „zatrudnił”

m.in. 20 robotów działających w 20 obszarach, w tym m.in. w zakresie księgowania kredytu i wypłaty środków”⁴⁴.

Bank Millennium

Bank Millennium w swojej „Strategii na lata 2022-2024”⁴⁵ zapowiada, że planuje **przy pomocy AI, wzmocnienie obsługi klienta, aby lepiej antycypować ich potrzeby i umożliwić lepsze spersonalizowanie oferty**.

Bank Millennium jest też kolejnym polskim bankiem, który **publikuje na swoich portalach społecznościowych wpisy z treściami o sztucznej inteligencji, promując wiedzę o tej technologii**

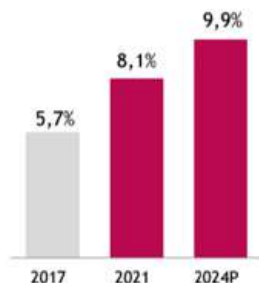
44 <https://www.bnpparibas.pl/blog/sztuczna-inteligencja-ai-i-zrobotyzowana-automatyzacja-procesow-pro-realia-i-przewidywania>, dostęp: 10 marca 2024 r.

45 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.bankmillennium.pl/documents/10184/123526/Millennium_Strategy2022-24_investorpresentation_PL.pdf?mv=2c, dostęp: 10 marca 2024 r.

Consumer Finance | Będziemy dalej wykorzystywać potencjał własnej bazy klientów i pozyskiwać nowych poprzez udoskonalony proces cyfrowy 46

W produktach consumer finance przekroczyliśmy nasz przeciętny udział w rynku i skupiamy się na dalszym rozwoju aby osiągnąć -10%...

Udział rynkowy w przychodach z CF (%)



Udział rynkowy w nowej produkcji / sprzedaży brutto¹



... poprzez inwestowanie w poprawę oferowanej wartości zarówno dla istniejącej bazy klientów, jak również nowo pozyskanych.

01 Nowo pozyskani klienci



Wsparcie poprzez PSD2 nowych możliwości weryfikacji dochodu, aby zapewnić sprawniejszą akwizycję klientów



Zaoferowanie rozwiązania w czasie i miejscu, w którym klient tego potrzebuje

02 Obecni klienci Banku



Dodanie nowych partnerów kredytów e-ratalnych i zwiększenie wielkości sprzedaży krzyżowej kredytów gotówkowych przy użyciu nowych, bardziej innowacyjnych rozwiązań cyfrowych



Wzmocnienie dzięki analityce danych AI, aby antycypować potrzeby klientów i umożliwić spersonalizowanie oferty

... i wsparcie oraz edukacja klienta



Wzmocnienie obsługi klienta przez stworzenie wysoce przyjaznych narzędzi kontaktu, głównie cyfrowych, i zwiększenie wiedzy klienta nt. produktu



Stąły rozwój CX we wszystkich kanałach, osiągnięty dzięki uproszczeniu procesów i premiowaniu szerszych kontaktów z Bankiem



Stymulowanie migracji prostych transakcji dot. kredyt. gotówkowych do kanałów cyfrowych, aby zwiększyć dostępność i satysfakcję klienta



1. W tym: kredyt gotówkowy, karta kredytowa, kredyt w rachunku bieżącym / 2. tpol. 21
Źródło: Bank Millennium, BCG Banking Value Pool Model

46 https://www.bankmillennium.pl/documents/10184/123526/Millennium_Strategy2022-24_investorpresentation_PL.pdf, dostęp: 10 marca 2024 r.

oraz „oswajając” z nią swoich klientów i innych odbiorców⁴⁷.

Na temat AI wypowiada się Halina Karpińska, Dyrektor Departamentu Bankowości Elektronicznej w Banku Millennium:



Bank Millennium
29 113 obserwujących
10 mies. • 🌐

+ Obserwuj ...48

Skuteczna adopcja AI w sektorze finansowym - jak etycznie wykorzystać potencjał Sztucznej Inteligencji i uniknąć ślepych zaułków? Podczas debaty na [Europejski Kongres Finansowy](#) eksperci z obszarów strategii, operacji, digital bankingu, a także danych i algorytmów mieli okazję opowiedzieć o praktycznych doświadczeniach wykorzystania AI w biznesie.

- Sztuczna inteligencja niewątpliwie może nam pomagać w wielu branżach, ale musimy być też świadomi jej zagrożeń. AI to sieć algorytmów i zaprojektowany model, który został zasilony danymi, w oparciu o które działa. Jeśli są to wyłącznie dane tendencyjne, wtedy też będzie rozprzestrzeniać informacje, które są tendencyjne, co może wpływać na przykład na tworzenie się baniek informacyjnych. Osobiście wierzę, że liczba zalet AI jest dużo większa niż potencjalnych ryzyk. Należy wyznaczyć linię pomiędzy dobrą, a złą stroną "mocy". Dlatego niezwykle istotna jest współpraca firm technologicznych, które rozwijają narzędzia AI z regulatorami oraz zdroworozsądkowe podejście w tworzeniu nowych oraz modyfikacja i otwartość dostosowania w obecnych regulacjach w odniesieniu do rozwoju narzędzi sztucznej inteligencji - powiedziała [Halina Karpińska](#), dyrektorka Dep. Bankowości Elektronicznej w Banku Millennium podczas debaty, której gospodarzem była firma [KPMG Poland](#).

W innym miejscu cytowana wyżej osoba tłumaczy:

„Rozwiązania oparte na AI pozwolą jeszcze lepiej obsługiwać klientów, dokładniej i szybciej analizować dane, a dzięki temu odpowiadać na potrzeby w czasie rzeczywistym i wzmocnić bezpieczeństwo. Dzięki AI będziemy mogli zapewnić wsparcie większej liczbie klientów w tym samym czasie, bez dodatkowego obciążenia pracowników banku. W Banku Millennium projekty związane z AI już trwają. Jeśli chodzi o trendy w płatnościach, to na pewno wciąż będzie rosła popularność rozwiązań typu wearables i biometrii użytkownika, ale także wszelkiego rodzaju mobilnych płatności”⁴⁹.

2.4. Wnioski

W świetle przeprowadzonej wyżej analizy, stwierdzić trzeba, że polskie banki mogą być nie tylko ocenione jako nowatorskie i zaangażowane technologicznie⁵⁰, ale – choć wdrażają je z ostrożnością i wyłącznie pod nadzorem czynnika ludzkiego – wykorzystują lub próbują wykorzystywać (poprzez testy) rozwiązania bazujące na sztucznej inteligencji praktycznie we wszystkich możliwych obszarach, tj.:

1. **tz. asystentów wirtualnych i chatboty** – czyli mechanizmy obsługi klientów w czasie rzeczywistym;
2. **antyfraudowe systemy bezpieczeństwa** – czyli mechanizmy weryfikacji transakcji w celu identyfikacji potencjalnych błędów lub oszustw;
3. **opcje personalizacji** – analiza danych klientów w celu dostarczenia jak najbardziej zindywidualizowanej, optymalnej oferty usługi;
4. **automatyczne doradztwo inwestycyjne (robo-doradztwo)** – automatyczne rekomendacje dotyczące inwestycji, bazujące na analizie danych;
5. **optymalizacja procesów operacyjnych** – automatyzacja rutynowych zadań (np. przetwarzanie dokumentów);
6. **analiza zachowań klientów;**
7. **systemy zarządzania ryzykiem;**
8. **biometryczne narzędzia uwierzytelniania** (czyli np. na podstawie uśmiechu, gestów, zachowań⁵¹);
9. **optymalizacja sieci oddziałów;**
10. **interaktywne panele informacyjne**⁵²,

47 https://www.linkedin.com/posts/bank-millennium_skuteczna-adopcja-ai-w-sektorze-finansowym-activity-7072138270813360129-v-Ty?utm_source=share&utm_medium=member_desktop, dostęp: 10 marca 2024 r.

48 https://www.linkedin.com/posts/bank-millennium_skuteczna-adopcja-ai-w-sektorze-finansowym-activity-7072138270813360129-v-Ty?originalSubdomain=pl, dostęp: 10 marca 2024 r.

49 M. Złoch, *Bankowość i Finanse | Technologie – Trendy | Sztuczna inteligencja i długo, długo nic*, „Miesięcznik Finansowy BANK” z 9 lutego 2024 r., <https://bank.pl/bankowosc-i-finanse-technologie-trendy-sztuczna-inteligencja-i-dlugo-dlugo-nic/>, dostęp: 10 marca 2024 r.

50 Co zresztą potwierdzają inni eksperci, wywodzący się również z innych środowisk niż sektor bankowy, np.: W. Boczoń, *Placówki bankowe nie znikną. Ale sztuczna inteligencja będzie obecna w każdym obszarze bankowości*, <https://www.bankier.pl/wiadomosc/Placowki-bankowe-nie-znikna-Ale-sztuczna-inteligencja-bedzie-obecna-w-kazdym-obszarze-bankowosci-8579152.html> dostęp: 10 marca 2024 r.

51 M. Jankowski, *Biometria z pudełka* [w:] Raport: Sztuczna inteligencja w bankowości, Warszawa 2020, s. 57.

52 *Sztuczna inteligencja w bankowości i inne innowacyjne rozwiązania dla sektora finansów*, <https://www.ironmountain.com/pl-pl/resources/blogs-and-articles/a/artificial-intelligence-in-banking-and-other-innovative-solutions-for-the-finance-sector>, dostęp: 10 marca 2024 r.

czyli rozwiązania służące zarówno wsparciu *front office*, jak i *back office*.

W tym sensie uzasadniona wydaje się bardzo optymistyczna ocena, zgodnie z którą: „**banki w Polsce, dzięki otwartości i sprawnej implementacji AI, stanowią obecnie dla innych sektorów punkt odniesienia pod względem dojrzałości technologicznej i innowacyjności**”⁵³.

Biorąc pod uwagę oceny prezentowane w wywiadach, a także poglądy formułowane w literaturze, nie można wykluczyć prawidłowości tezy, że to właśnie szeroko rozumiany sektor finansowy najmocniej skorzysta z rozwiązań opartych na sztucznej inteligencji⁵⁴.

W świetle przeprowadzonych rozmów, potwierdza się również wniosek, iż reprezentanci sektora bankowego z niecierpliwością, lecz jednocześnie z pewną obawą, czekali na regulacje unijne (zwłaszcza AI ACT), które przesądzą jakie konkretnie rozwiązania mogą być stosowane, na jakich warunkach, jakie natomiast obarczone są ryzykiem i niebezpieczeństwem narażenia na sankcje, roszczenia odszkodowawcze itp.⁵⁵.

Wydaje się, że respondenci oraz inni reprezentanci sektora bankowego – w ocenach sztucznej inteligencji oraz jej wdrożeniach – zachowują jednocześnie pożądaną ostrożność, dystans, przyjmując postawę umiarkowania zachowawczą, by minimalizować ryzyka. Co więcej, odnieść można wrażenie, że nawet obecnie – mimo faktycznej deregulacji licznych obszarów związanych z AI – trafnie identyfikują ryzyka, unikając takich zastosowań AI, które mogłyby wchodzić w konflikt z prawami człowieka i indywidualnymi wolnościami, a także zapobiegać dyskryminacji, stronnictwu, a zapewnić wyjaśnialność i przejrzystość tych narzędzi⁵⁶.

Ci z respondentów, którzy zdecydowali się nawiązać w swych wypowiedziach do regulacji prawnej, wyrażali wątpliwości związane z prawnym zdefiniowanym sztucznej inteligencji. Podobne stanowisko prezentują często prawnicy⁵⁷. Z drugiej strony, raczej pozytywnie oceniana była koncepcja ujednolicenia regulacji na poziomie unijnym, zamiast utrzymywania niekonsekwentnych rozwiązań na szczeblu krajowym⁵⁸. Zwłaszcza, że – jak wskazuje się w literaturze – brak jasnych i przejrzystych, nie budzących wątpliwości aktów prawnych pozwalających na bezpieczne i pewne posługiwanie się sztuczną inteligencją w działalności bankowej, jest właśnie jedną z podstawowych przeszkód w jej rozwoju⁵⁹. Podkreślano również konieczność wyważenia różnych zasad konstytucyjnych oraz interesów, w tym zwłaszcza troski o sytuację jednostki (zwłaszcza słabszego klienta, konsumenta), z koniecznością rozwoju technologicznego i optymalizacji procesów bankowych⁶⁰. Niektórzy z respondentów wyrażali również pogląd, że na rozwój instytucji finansowych negatywnie wpływa zarówno brak, jak i nadmiar regulacji⁶¹.

Mimo towarzyszących AI ACT nadziei, większość respondentów nie ma złudzeń, że – niezależnie od szczegółowości regulacji unijnej – konieczne będzie dostosowanie krajowego stanu prawnego do tej zmiany, a kluczowa rola nie musi wcale przypaść ustawodawcy, ale polskim organom władzy publicznej uprawnionym do władczego rozstrzygania, wydawania decyzji administracyjnych lub rekomendacji (KNF). Uczestnicy wywiadów zasadniczo zgadzają się zatem z poglądem, według którego „niekiedy prawodawstwo nie nadąża za rozwojem technologicz-

53 *Sztuczna inteligencja w bankowości: polski sektor na czele*, https://managerplus.pl/sztuczna-inteligencja-w-bankowosci-polski-sektor-na-czele-87526#google_vignette, dostęp: 10 marca 2024 r.

54 *Nadchodzi era AI: jak sztuczna inteligencja zmienia bankowość*, „Puls Biznesu” z dnia 28 czerwca 2023 r., <https://www.pb.pl/nadchodzi-era-ai-jak-sztuczna-inteligencja-zmienia-bankowosc-1189108>, dostęp: 10 marca 2024 r.

55 T. Jurczak, *Jak AI wpłynie na sektor bankowy?*, „Dziennik Gazeta Prawna” z dnia 15 grudnia 2023 r., <https://serwisy.gazetaprawna.pl/ai-w-biznesie/artykuly/9382432,jak-ai-wplynie-na-sektor-bankowy-wywiad.html>, dostęp: 10 marca 2024 r.

56 M. Sakowska-Baryła, *Standardy etyczne przy wykorzystywaniu sztucznej inteligencji* [w:] *Prawo sztucznej inteligencji i nowych technologii*, B. Fischer, A. Pązik, M. Świerczyński (red.), Warszawa 2023.

57 P. Staszczuk, *Czy unijna regulacja odpowiedzialności cywilnej za sztuczną inteligencję jest potrzebna?*, „Europejski Przegląd Sądowy”, 6/2022, s. 24-30; M. Nowakowski, *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023, s. 23.

58 Na ten temat zob.: K. Rębisz, *Wybrane zagadnienia prawa cywilnego w propozycjach regulacyjnych dotyczących sztucznej inteligencji w Unii Europejskiej*, „Europejski Przegląd Sądowy”, 10/2021, s. 22-27.

59 D. Ślażyńska-Kluczek, *Sztuczna inteligencja – regulacje prawne, miejsce w polskim sektorze bankowym*, „Nauki Ekonomiczne”, 34(5)/2021, s. 67.

60 Na ten temat zob. też: J. Mazur, *Unia Europejska wobec rozwoju sztucznej inteligencji: proponowane strategie regulacyjne a budowanie jednolitego rynku cyfrowego*, „Europejski Przegląd Sądowy”, 9/2020, s. 13-18; P. Kusznieruk, *Wpływ rozwoju sztucznej inteligencji na proces stanowienia prawa w Polsce*, „Przegląd Prawa Publicznego”, 5/2023, s. 12-13.

61 Zob. też: W. Bożek, *Informatyzacja rynku usług finansowych na przykładzie sektora usług płatniczych i bankowych* [w:] *Prawo nowych technologii*, K. Flaga-Gieruszyńska, J. Gołaczyński (red.), Warszawa 2021, s. 185.

nym, pojawiają się duże wyzwania przy implementacji takich rozwiązań”⁶².

Podkreślić trzeba, że **respondenci zdają się trafnie identyfikować największe związane z AI ACT zagrożenia i ryzyka, a nawet intuicyjnie wyczuwać rozwiązania wrażliwe, potencjalnie problematyczne, narażające bank na sankcje, kary, roszczenia odszkodowawcze (m.in. dotyczące naruszania przepisów o danych osobowych, zbierające i wykorzystu-**

jące niektóre wrażliwe dane biometryczne, badające zdolność kredytową z potencjalnym naruszeniem obowiązujących zasad, w tym wyjaśnialności).

Uczestnicy badania byli również świadomi faktu, że działalność instytucji finansowych poza rynkiem unijnym, zwłaszcza w Azji, pozostaje na ogół słabiej (mniej restrykcyjnie) uregulowana, co sprzyja innowacyjności, lecz niekoniecznie sprzyja wysokiemu poziomowi ochrony konsumenta⁶³.

62 M. Nowakowski, *FINTECH - technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2020, s. 181–182.

63 M. Dziedzic, *Ochrona konsumenta w związku z zagrożeniami płynącymi z rozwoju FinTech* [w:] T. Szancito (red.), *Prawna ochrona konsumenta rynku usług bankowych*, Warszawa 2023, Legalis.

3. Przegląd doświadczeń zagranicznych





3.1. Wprowadzenie

Zastanawiając się nad aktualnymi wyzwaniami prawnymi związanymi z zastosowaniem sztucznej inteligencji w polskim systemie bankowym nie sposób oderwać się tak od rozwiązań technicznych istniejących i stosowanych, jak i **regulacji prawnych przyjętych przez inne państwa, w tym zarówno państwa członkowskie Unii Europejskiej, jak również państwa, których kultura prawna odmienna jest od rodzimej**. Wydaje się bowiem, że globalny zasięg rozwiązań technologicznych, o których mowa w niniejszym raporcie, otwiera szerokie pole do dyskusji na płaszczyźnie ponadnarodowej.

Kształtowanie się nowej gałęzi prawa – prawa nowych technologii⁶⁴, czy też jak się niekiedy wskazuje jeszcze bardziej zawężająco prawa sztucznej inteligencji⁶⁵, jest obecnie faktem. Świadczy o tym chociażby istotny i stały rozrost literatury przedmiotu, w tym również obserwowany przyrost liczby czasopism naukowych poświęconych tejże problematyce⁶⁶. Należy jednak również odnotować, że zainteresowanie przedmiotową problematyką występowało już nawet ponad pół wieku temu. W roku 1970 powstało czasopismo naukowe poświęcone tematyce sztucznej inteligencji – *Artificial intelligence*. Z kolei w 1992 r. powstało inne czasopismo, które zajmowało się zagadnieniami na styku AI oraz prawa – *Artificial intelligence and law*⁶⁷.

Wprawdzie raport dotyczy zagadnień związanych z sektorem bankowym, to jednak stwierdzić należy, że rozwiązania właściwe dla sektora bankowego każdorazowo będą musiały mieścić się w rozwiązaniach ogólnych, tj. w ogólnych uregulowaniach prawnych, w tym w szczególności ustawodawczych. Wobec tego niezbędne będzie przeprowadzenie analizy

regulacji prawa nowych technologii zarówno z perspektywy polskiej, jak i z perspektywy obcej.

Prawo z jednej strony reguluje istniejącą rzeczywistość, z drugiej zaś stanowi ramy dla stale rozwijającej się rzeczywistości, przewidując jak rozwój ten może wyglądać. Stąd regulacje dotyczące sztucznej inteligencji, w tym jej wykorzystania w sektorze bankowym stanowią po pierwsze uregulowanie istniejących już zagadnień powstałych wraz z rozwojem AI, po wtóre zaś wytyczają granice, w jakich AI może być rozwijana. Niekiedy granice te będą miały charakter ogólny, innym razem zaś bardziej sektorowy. Wydaje się, że jednym z kluczowych – choć jak wykaże zaprezentowana analiza prawnoporównawcza, kwestia ta nie jest jeszcze przez prawodawców szczegółowo regulowana – rozstrzygnięć legislacyjnych będzie ustalenie reguł odpowiedzialności za szkodę wyrządzoną przez AI, lub jej nieprawidłowe działanie⁶⁸.

Użycie prawa polegać też może na **minimalizowaniu, rozpoznawalnych i negatywnie wartościowanych przez system prawa, skutków zastosowania AI nie stanowiących szkody w rozumieniu prawa cywilnego**. W szczególności do tego typu ingerencji należeć będzie ustanawianie szczegółowych, niekiedy *strictie* technicznych, reguł postępowania w odniesieniu do tworzonych w przyszłości systemów sztucznej inteligencji. Wśród istotnych ograniczeń technologicznych AI odnotować należy m.in. **problem dyskryminacji automatycznej, czy też przejrzystości procesów rządzących działaniem sztucznej inteligencji**.

Aby możliwe było zrealizowanie założeń postawionych przy tworzeniu niniejszego raportu, wobec powyższych uwag należało przeprowadzić analizę porównawczą, w tym w szczególności prawnoporównawczą. Przyjęcie perspektywy komparatystycznej w odniesieniu do doświadczeń zagranicznych w sposób naturalny prowadzi do ujęcia omawianej kwestii z perspektywy poszczególnych dyskursów krajowych, a także sygnalizowanych wcześniej oddziaływań występujących pomiędzy krajowymi systemami prawa.

64 O stopniowym wyodrębnianiu się prawa nowych technologii jako autonomicznej gałęzi prawa świadczy m.in. powstawanie opracowań naukowych poświęconych tej tematyce. Zob. O stopniowym wyodrębnianiu się prawa nowych technologii jako autonomicznej gałęzi prawa świadczy m.in. powstawanie opracowań naukowych poświęconych tej tematyce. Zob. A. Arkuszewska et al., *Prawo nowych technologii*, K. Flaga-Gieruszyńska i J. Gołaczyński (red.), Warszawa 2021.

65 Zob. L. Lai, M. Świerczyński, *Wstęp* [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, s. LIX–L, czy B. Fischer, A. Pązik, M. Świerczyński (red.), *Prawo sztucznej inteligencji i nowych technologii*, Warszawa 2021, gdzie już w samym tytule widać oba wskazane pojęcia.

66 Warto wskazać przykładowo na wydawany przez C.H. Beck od r. 2021 kwartalnik *Prawo Nowych Technologii*.

67 T. Zalewski, *Definicja sztucznej inteligencji* [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, s. 3.

68 Problemy te w kontekście ogólnym były już poruszane w nauce. Zob. M. Wałachowska, *Sztuczna inteligencja a zasady odpowiedzialności cywilnej* [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, s. 57 i n. oraz M. Jagielska, *Odpowiedzialność za sztuczną inteligencję* [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, s. 69 i n.

W pierwszej kolejności, ze względu na mnogość podejmowanych działań oraz ich zróżnicowany charakter, przybliżone zostaną postępy w regulacji sztucznej inteligencji charakterystyczne dla systemu prawnego Stanów Zjednoczonych Ameryki (dalej jako: USA). Również obserwowana intensyfikacja kolejnych przedsięwzięć legislacyjnych oraz coraz wyższa jakość tworzonych przepisów wskazuje na zasadność rozpoczęcia przeglądu doświadczeń zagranicznych właśnie od USA.

Szczególną uwagę warto również poświęcić inicjatywie prawodawczej podjętej w Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej (dalej również jako: UK). Przyjęty **model stanowienia prawa, przynajmniej w odniesieniu do prawa nowych technologii, zakłada przeprowadzenie szerokich konsultacji społecznych, w tym z ekspertami, w oparciu o dokument (tzw. „white paper”) zarysowujący pożądane skutki oraz podstawowe założenia projektowanej regulacji**. Podobnie, jak ma to miejsce w przypadku USA, UK przynależy do tradycji prawnej *common law*. Z tego względu rozwój regulacji w tych państwach może stanowić tło dla naświetlenia dorobku państw tradycji prawa kontynentalnego (tzw. „continental law” lub „civil law”).

Za **przykład prawodawstw funkcjonujących w ramach tej tradycji prawnej obrano dorobek prawny Republiki Francuskiej oraz Republiki Federalnej Niemiec**. Państwa te, wypracowały szereg szczegółowych rozwiązań, których skonfrontowanie pozwoli na uwypuklenie istotnych cech aktualnych wyzwań prawnych związanych z wykorzystaniem AI w bankowości. Warto wspomnieć, że pomimo podkreślenia autonomii obu ww. systemów prawnych, w tożsamym stopniu spełniać one muszą standardy wynikające z norm rangi unijnej. Akty normatywne o pierwszorzędym znaczeniu dla niniejszej dyskusji przedstawione zostaną w dalszej części przedmiotowego raportu (zob. rozdział IV), natomiast warto już w tym miejscu zaznaczyć, że wszelkie postulowane na poziomie krajowym rozwiązania prawne będą musiały realizować wymogi stawiane przez prawodawstwo unijne.

Na zakończenie analizy prawnoporównawczej w obszarze zainteresowań znajdzie się państwo azjatyckie, jakim jest **Chińska Republika Ludowa (dalej jako: Chiny)**. W kraju tym **nowoczesne technologie, w tym systemy sztucznej inteligencji, charakteryzują się niezwykle dynamicznym, wręcz pionierskim rozwojem**. Za rozwojem tym podążają również regulacje prawne. Z uwagi jednak na ograniczenia

natury faktycznej w dostępie do chińskich regulacji mogą one zostać omówione jedynie w ogólny sposób, przybliżający ich istotę. Stąd przykład ten jako pewnego rodzaju ciekawe rozwiązanie omówiony zostanie w ostatniej kolejności.

W tej perspektywie sięgnięcie do dorobku jurysprudence wywodzących się z tak różnych tradycji prawnych posłużyć może realizacji funkcji prawotwórczej analizy komparatystycznej⁶⁹. W analizach poszczególnych porządków prawnych zwrócona zostanie szczególna uwaga na wyspecjalizowane podmioty, znane pod zbiorczym pojęciem regulatorów krajowych, tudzież regulatorów sektorowych, powołane w celu tworzenia pewnego rodzaju **rekomendacji w określonych obszarach**. **Wydane przez nie akty prawne będą zatem miały charakter źródeł prawa soft law**, jednak uwzględnianie ich treści w podejmowanych działaniach przez zainteresowane podmioty może mieć silniejszy charakter od zwykłej rekomendacji. Mowa tu w szczególności o takich podmiotach jak działający w USA Narodowy Instytut Standaryzacji i Technologii (*National Institute of Standards and Technology*; dalej jako: NIST)⁷⁰, francuska Komisja Narodowa ds. Informatyki i Wolności (*Commission Nationale de l'Informatique et des Libertés*; dalej jako: CNIL), działający w UK Urząd ds. Postępowania Finansowego (*Financial Conduct Authority*; dalej jako: FCA), czy niemiecki organ nadzoru nad rynkiem finansowym (niem. *Bundesanstalt für Finanzdienstleistungsaufsicht*, dalej jako: BaFin).

3.2. USA

Ostatnimi czasy w USA obserwowalna jest **znaczna intensyfikacja wysiłków legislacyjnych – zarówno na poziomie federalnym, jak i stanowym – nakierowanych na utworzenie ram dla dalszego rozwoju AI**. Za szczególnie doniosłą deklarację uznać należy rozporządzenie wykonawcze Prezydenta USA z dnia 30 października 2023 r. w sprawie bezpiecznego i godnego zaufania rozwoju i wykorzystania sztucznej inteligencji (*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*)⁷¹.

69 Zob. R.A. Tokarczyk, *Komparatystyka prawnicza*, Wolters Kluwer Polska, Warszawa 2008, 9. wyd., s. 204–205.

70 Tu i dalej, o ile nie zostało zaznaczone inaczej, tłumaczenie autorskie.

71 <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>, dostęp: 9 grudnia 2023 r.



Wskazany akt normatywny stanowi nie tylko zapowiedź dalszych prac ustawodawcy federalnego, ale definiuje również podstawowe cechy kształtowanego modelu regulacji AI. **Założenia te można podsumować w następujący sposób:**

1. **nowe standardy bezpieczeństwa AI:** rozporządzenie zobowiązuje twórców systemów sztucznej inteligencji do udostępniania rządowi wyników testów bezpieczeństwa, a nadto przewiduje ustanowienie podstawowych standardów, narzędzi i testów bezpieczeństwa dla systemów sztucznej inteligencji oraz koncentruje się na **zagrożeniach związanych z wykorzystaniem AI dla infrastruktury krytycznej państwa**;
2. **ochrona prywatności obywateli:** rozporządzenie wzywa Kongres Stanów Zjednoczonych do przyjęcia przepisów dotyczących **ochrony danych osobowych**, gwarantuje federalne wsparcie dla **rozwoju technik ochrony prywatności** w wykorzystaniu sztucznej inteligencji oraz deklaruje zapewnienie **mechanizmu oceny, w jaki sposób agencje rządowe gromadzą i wykorzystują informacje**;
3. **promowanie równości społecznej:** rozporządzenie deklaruje podjęcie prac nad określeniem katalogu wytycznych mających na celu **zapobieganie pogłębianiu zjawiska dyskryminacji automatycznej oraz przeciwdziałanie jej skutkom poprzez szkolenia i odpowiednią koordynację działań**, a także postuluje zapewnienie sprawiedliwości w toku stosowania AI przez organy wymiaru sprawiedliwości;
4. **ochrona konsumentów, pacjentów i studentów:** rozporządzenie koncentruje się na promowaniu odpowiedzialnego wykorzystania sztucznej inteligencji w opiece zdrowotnej, kształtowaniu potencjału sztucznej inteligencji w edukacji i **ochronie konsumentów przed potencjalnymi szkodami i innymi nadużyciami** ze strony przedsiębiorców wykorzystujących AI;
5. **zapewnienie bezpieczeństwa pracowników:** z wykorzystaniem sztucznej inteligencji w miejscu pracy związane jest ryzyko nadużyć, a jego minimalizacja powinna polegać przede wszystkim na utworzeniu katalogu zasad oraz dobrych praktyk w odniesieniu do kształtowania sytuacji pracowników; rozporządzenie zleca ponadto **sporządzenie raportu na temat – rzeczywistego i potencjalnego – wpływu sztucznej inteligencji**

na rynek pracy oraz wzmocnienie federalnego systemu wsparcia dla pracowników poszkodowanych przez funkcjonowanie AI;

6. **rozpowszechnianie innowacyjności i konkurencyjności:** kluczowe jest zapewnienie warunków dla przyspieszenia badań nad sztuczną inteligencją, a także wytworzenie sprawiedliwego i konkurencyjnego „ekosystemu” sztucznej inteligencji oraz zwiększenie możliwości studiowania, pobytu i pracy w USA dla osób mogących przyczynić się do rozwoju AI w USA;
7. **globalizacja:** rozporządzenie wzywa do **międzynarodowej współpracy w zakresie sztucznej inteligencji**, przyspieszenia prac nad określeniem standardów stawianych przed systemami sztucznej inteligencji oraz zapewnienia odpowiedzialnego rozwoju i mechanizmów wdrażania sztucznej inteligencji na całym świecie;
8. **zapewnienie odpowiedzialnego i skutecznego wykorzystania sztucznej inteligencji przez rząd USA:** postulowane środki obejmują wydanie wytycznych dotyczących wykorzystania sztucznej inteligencji, poprawę mechanizmu zamawiania i wdrażania systemów sztucznej inteligencji oraz **przyspieszenie zatrudniania specjalistów ds. sztucznej inteligencji w agencjach rządowych**.

Wspomniane rozporządzenie wykonawcze nakłada również pewne obowiązki na NIST. Warto odnotować, że termin realizacji większości zleconych w rozporządzeniu wykonawczym zadań określono jako 270 dni (zadania te zatem powinny zostać zrealizowane w istocie do początku sierpnia 2024 r.), co obrazuje znaczną obecną i przyszłą dynamikę prac nad uregulowaniem statusu prawnego zjawiska sztucznej inteligencji oraz jej szerszego kontekstu socjo-ekonomicznego. Godne podkreślenia jest **szerokie pole działalności NIST**. Prace tej agencji obejmują swym zakresem po pierwsze przygotowanie raportu podsumowującego aktualny stan wiedzy oraz identyfikację dobrych praktyk dotyczących m.in.: uwierzytelniania treści i śledzenia jej pochodzenia; metod oznaczania (np. z wykorzystaniem tzw. „znaku wodnego”) treści wygenerowanych za pośrednictwem AI; metod wykrywania treści wygenerowanych z wykorzystaniem AI; zapobiegania generowaniu przez sztuczną inteligencję materiałów przedstawiających seksualne wykorzystywanie dzieci lub tworzenia zdjęć prawdziwych osób bez ich zgody; testowa-

nia oprogramowania wykorzystywanego do powyższych celów. Po drugie, NIST opracować ma wytyczne oraz rozwiązania wspierające wdrażanie podstawowych praktyk zarządzania ryzykiem generowanym przez AI. Po trzecie, agencja ta udzieli Sekretarzowi Handlu wsparcia w ramach dialogu z kluczowymi partnerami międzynarodowymi i organizacjami opracowującymi standardy dotyczących wykorzystywania AI w celu stymulowania rozwoju sztucznej inteligencji oraz pogłębiania współpracy i wymiany informacji w tym zakresie. Wszystkie zadania realizowane będą przy udziale sektora prywatnego, środowiska akademickiego i uwzględniać mają potrzeby społeczeństwa obywatelskiego⁷².

Warto nadmienić, że szereg inicjatyw związanych ze sztuczną inteligencją został podjęty przez NIST jeszcze przed wydaniem przedmiotowego rozporządzenia wykonawczego. Przykładowo, już w styczniu 2023 r. opublikowano **dokument pt. „Ramy zarządzania ryzykiem związanym ze sztuczną inteligencją” (Artificial Intelligence Risk Management Framework; dalej jako: AI RMF)**⁷³. Charakteryzuje on zarówno czynniki mogące odgrywać istotną rolę w ocenie ryzyka związanego z wykorzystaniem AI, jak i wymogi brzegowe uznania systemu sztucznej inteligencji za godny zaufania. Wydaje się, że drugie z wymienionych zagadnień stanowić może ważne wskazanie dla praktyki wykorzystania AI w sektorze bankowym. Warto już w tym miejscu zaznaczyć, że zaprezentowany poniżej zestaw koresponduje z ustaleniami poczynionymi przez specjalistów z zakresu SI w ostatnich latach. W tym zakresie AI RMF stanowi zwięzłe podsumowanie aktualnego stanu wiedzy oraz próbę przełożenia postulatów naukowych na praktykę tworzenia i funkcjonowania AI. Z tych względów, a także mając na uwadze znaczenie zapewnienia w sektorze bankowym najwyższych możliwych standardów, w ocenie autorów niniejszego raportu uzasadnione jest szersze przedstawienie elementów charakteryzujących godne zaufania systemy sztucznej inteligencji.

Podstawowymi postulowanymi w AI RMF cechami godnego zaufania AI są jego **prawidłowość (validity)** i **niezawodność (reliability)**. Kryteria te powinny

być rozumiane łącznie jako trwała dyspozycja do działania, w ramach określonego sposobu użycia, zgodnie z zamiarem twórców. Kontrola systemu sztucznej inteligencji w odniesieniu do tych, stanowiących warunek konieczny uznania systemu SI za godny zaufania, cech polegać może w szczególności na zapewnieniu ciągłego nadzoru nad sposobem funkcjonowania systemu.

W dalszej kolejności parametrem określającym stopień zaufania do AI jest **zapewnianie przezeń bezpieczeństwa użytkownikom systemu (safety)**. System sztucznej inteligencji nie może zagrażać życiu lub zdrowiu użytkownika oraz nie powinien naruszać jego prawa własności lub szkodzić środowisku naturalnemu.

System sztucznej inteligencji powinien także **wykazywać się odpornością na zagrożenia zewnętrzne, tj. próby jego nadużycia (security)**. W szczególności AI powinno posiadać mechanizmy zapobiegające różnego rodzaju atakom (np. zatrucie danych lub eksfiltracja modelu SI), metody ograniczania rozmiarów szkód spowodowanych nieprawidłowym wykorzystaniem AI oraz **sposoby przywrócenia prawidłowego działania SI (resilience)**.

Rozliczalność (accountability) i przejrzystość (transparency) systemu sztucznej inteligencji stanowią kolejną parę cech zwiększających poziom zaufania do AI. Przez przejrzystość należy rozumieć zakres, w jakim informacje o sposobie działania systemu sztucznej inteligencji i mechanizmie powstawania danych wyjściowych są dostępne dla osób wchodzących w interakcję z takim systemem. Z kolei rozliczalność stanowi pochodną przejrzystości, wszak ocena generowanej przez AI treści przez pryzmat zakładanych przez twórców mechanizmu działania SI wymaga jawności nie tylko tych założeń, ale również rzeczywistego sposobu działania AI.

Godny zaufania system sztucznej inteligencji musi ponadto cechować **wyjaśnialność (explainability) oraz interpretowalność (interpretability) rezultatów jego działania**⁷⁴. Wyjaśnialność rezultatu znaczy tyle, co łatwość z jaką przychodzi uzasadnienie konkretnego wyniku (wobec konkretnych danych

72 Szerzej zob. <https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence>, dostęp: 12 grudnia 2023 r.

73 <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>, dostęp: 13 grudnia 2023 r.

74 Jedynie na marginesie zaznaczyć można, że w piśmiennictwie niekiedy utożsamia się obie te cechy. Przykładowo zob. W. Buczyński et al., *Hard Law and Soft Law Regulations of Artificial Intelligence in Investment Management*, „Cambridge Yearbook of European Legal Studies”, 24/2022, s. 275.

wejściowych) w świetle sposobu działania danego systemu SI. Natomiast, interpretowalność rezultatu oznacza stopień, w jakim człowiek jest w stanie przewidzieć wygenerowanie tegoż rezultatu⁷⁵.

Równie istotną charakterystyką SI jest **ochrona prywatności użytkowników systemu** (*privacy-enhanced*). W tym świetle AI musi chronić możliwość wyrażania przez użytkowników zgody na ujawnianie i dalsze przetwarzanie elementów związanych z ich tożsamością (jak np. dane personalne czy wizerunek)⁷⁶.

O systemie sztucznej inteligencji można powiedzieć, że jest **sprawiedliwy (fair) wtedy, gdy minimalizuje ryzyko dyskryminacji automatycznej**. Określone zostały trzy główne kategorie zniekształceń prowadzących do dyskryminacji automatycznej. Są to kolejno zniekształcenia systemowe, obliczeniowo-statystyczne oraz poznawcze. Zniekształcenia systemowe dotyczą nie tylko zbiorów danych używanych przez AI, ale również norm organizacyjnych, praktyk i procesów związanych z wykorzystaniem systemów AI. Zniekształcenia obliczeniowo-statystyczne mogą być obecne w zbiorach danych AI i procesach algorytmicznych i często wynikają z błędów systematycznych spowodowanych uwzględnieniem w zbiorze próbek niereprezentatywnych. Zniekształcenia poznawcze odnoszą się do sposobu, w jaki dana osoba lub grupa postrzega treści generowane przez system AI, lub do sposobu, w jaki użytkownicy myślą o celach i funkcjach wykorzystywanego przez nich AI.

Problematyka sztucznej inteligencji w pracach NIST nie zamyka się jedynie w ramach określenia, jakimi właściwościami powinny cechować się systemy AI. Działalność tejże agencji obejmuje również, w zakresie rozwoju AI, **publikację szeregu innych opar-**

cowań tematycznych⁷⁷, organizowanie warsztatów poświęconych zagadnieniom praktycznym, czy zapewnianie obsługi grantów badawczych.

Powyższe nie oznacza jednak, że prace legislacyjne nie obejmują, wstępnych chociaż, propozycji regulacji powszechnie obowiązującej. Przykładem aktywności prawodawcy federalnego jest w tym zakresie m.in. opublikowanie projektu ustawy o prawach związanych z wykorzystywaniem sztucznej inteligencji (*Blueprint for an AI Bill of Rights*)⁷⁸. Projekt ten – odnosząc się m.in. do AI RMF – przewiduje ustalenie katalogu praw, które mogą zostać opisane w następujący sposób:

1. **prawo do bezpiecznego i skutecznego AI:** system sztucznej inteligencji musi zapewniać bezpieczeństwo jego użytkownikom oraz działać w sposób zgodny z założeniami jego twórców, którzy powinni minimalizować ryzyko wykorzystania systemu SI w sposób niezgodny z przyjętymi założeniami;
2. **prawo do ochrony przed dyskryminacją automatyczną:** systemy sztucznej inteligencji muszą realizować swoje zadania w sposób sprawiedliwy. Bariery chroniące społeczeństwo przed dyskryminacją w codziennym życiu powinny obejmować również aktywność realizowaną w domenie cyfrowej;
3. **prawo do prywatności:** AI powinno gromadzić wyłącznie dane ściśle niezbędne w kontekście użycia określonego systemu sztucznej inteligencji, a zakres gromadzonych danych powinien odpowiadać uzasadnionym przewidywaniom użytkowników systemu sztucznej inteligencji;
4. **prawo do informacji:** obejmuje ono prawo jednostki do bycia poinformowanym o tym, że system sztucznej inteligencji został wykorzystany w toku oceny okoliczności istotnych dla załatwienia danej sprawy (niezależnie od jej charakteru prawnego), jak również prawo do uzyskania informacji w jaki sposób ocena dokonana przez AI miała przełożenie na kierunek załatwienia sprawy;

⁷⁵ Szerzej o zależnościach między wyjaśnialnością i interpretowalnością zob. A. Erasmus, T.D.P. Brunet, i E. Fisher, *What is Interpretability?*, „Philosophy & Technology”, 2021, t.34, nr 4, s. 833–862; K. Främling, *Decision Theory Meets Explainable AI*, „Explainable, Transparent Autonomous Agents and Multi-Agent Systems”, Springer International Publishing, Cham 2020, s. 57–74; R. Marcinkevičs i J.E. Vogt, *Interpretable and explainable machine learning: A methods-centric overview with concrete examples*, „WIREs Data Mining and Knowledge Discovery”, 3(13)/2023, s. 1–32.

⁷⁶ Zagadnienie ochrony prywatności użytkowników systemów AI jest w literaturze prawniczej, szczególnie europejskiej, szeroko dyskutowane. Ma to związek z wpływem, szerzej opisanego w dalszej części niniejszego raportu, prawodawstwa unijnego. Przykładowo zob. R. Dumnica i D.M. Ilie, *Ethical and legal aspects of the development and use of robotics and AI*, „Journal of Law and Administrative Sciences”, 2023, t.19, s. 26–27, 37.

⁷⁷ Tytułem przykładu zob. R. Schwartz et al., *Towards a standard for identifying and managing bias in artificial intelligence*, National Institute of Standards and Technology (U.S.), Gaithersburg, MD 2022, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf>.

⁷⁸ <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>, dostęp: 15 grudnia 2023 r.

5. **prawo do rezygnacji:** jednostka powinna mieć możliwość odstąpienia, w stosownych przypadkach, od załatwienia sprawy w sposób zautomatyzowany oraz mieć dostęp do alternatywnych, np. uwzględniających czynnik ludzki, mechanizmów oceny stanu faktycznego zachodzącego w jej sprawie.

Powyższy katalog praw, chociaż nie jest długi, to **z uwagi na jego nieostre sformułowanie ujęty jest szeroko i w przypadku chęci jego przeniesienia do regulacji prawnych wymagałby z pewnością pewnych wyjaśnień, czy uściśleń**. Nie został on jednak skonstruowany w oderwaniu od realnie występujących problemów w wykorzystaniu systemów sztucznej inteligencji oraz stosowaniu prawa w odniesieniu do nich, co obrazuje zaprezentowany poniżej przegląd najistotniejszych przypadków, w których widoczne są niedociągnięcia w zakresie funkcjonowania systemów AI.

Case study 1

Jak pokazuje praktyka, możliwa jest sytuacja nieprawidłowego działania systemu AI, które to działanie przekłada się na powstanie szkody lub nawet krzywdy po stronie konsumentów. Firma Rite Aid, która prowadzi sieć sklepów w USA, wykorzystywała technologię rozpoznawania twarzy do profilowania osób, które wcześniej uznała za skłonne do popełnienia kradzieży. **Technologia ta generowała alerty wysyłane do pracowników Rite Aid, w tym za pośrednictwem wiadomości e-mail lub powiadomień w aplikacji na telefon komórkowy, wskazujące, że osoby, które weszły do sklepów sieci Rite Aid, pasowały do wpisów w bazie danych osób wytypowanych do popełnienia przestępstwa kradzieży**. Podejmowanie przez pracowników Rite Aid działań – na podstawie fałszywych ostrzeżeń o wysokim stopniu dopasowania wizerunku konsumenta wchodzącego do sklepu z wizerunkiem utrwalonym w bazie danych – potencjalnie narażało konsumentów m.in. na ograniczenie możliwości dokonywania potrzebnych zakupów, poważny stres, uszczerbek na reputacji, a nawet prowadzić mogło do niesłusznego aresztowania. Wobec powyższych mankamentów, Federalna Komisja Handlu wystąpiła z powództwem o wydanie wobec Rite Aid nakazu wdrożenia stosownych mechanizmów ograniczających potencjalnie szkodliwe następstwa użycia AI⁷⁹. Co jednak

widoczne w tej sprawie, a niezwykle istotne to fakt, że pomimo istotnych niedociągnięć nie próbuje się wymusić na właścicielu systemu zaniechania jego używania, czy też innego odejścia od stosowanego systemu. Pokazuje to, że rozwój sztucznej inteligencji w codziennym życiu jest nieodczynnym i nie sposób jakkolwiek go hamować. Należy jedynie stworzyć takie przepisy i takie wymogi, aby systemy te działały na rzecz człowieka i starać się wyeliminować potencjalne zagrożenia z nich wynikające.

Case study 2

Istotnym wyzwaniem stojącym przed sektorem bankowym jest minimalizacja dyskryminacji automatycznej. Zwraca się uwagę w szczególności na potencjalne niebezpieczeństwa związane z wykorzystaniem AI w procesie oceny wiarygodności kredytowej danego podmiotu. Wskazać w tym zakresie można przykład działalności spółki Upstart Holdings Inc. (dalej jako: Upstart)⁸⁰. Spółka ta oferuje usługę internetowej platformy pożyczkowej, która kojarzyć ma ze sobą potencjalnych kredytobiorców oraz banki i spółdzielcze kasy oszczędnościowo-kredytowe współpracujące z Upstart. Platforma wykorzystuje **sztuczną inteligencję w procesie oceny zdolności kredytowej danego podmiotu uwzględniając zmienne uznawane za „nietradycyjne”, jak np. wykształcenie i historia zatrudnienia**. Jak zaznaczył Upstart, wykorzystywany model oceny zdolności kredytowej identyfikuje tzw. „niewidzialnych kredytobiorców” – tj. kredytobiorców, którym na podstawie standardowych wskaźników⁸¹, albo odmówiono by udzielenia kredytu, albo udzielono by go na niekorzystnych warunkach – oraz zwiększa ich szanse na uzyskanie kredytu, przyczyniając się tym samym do zmniejszania różnic w dostępie do usług finansowych.

W 2020 r. Centrum Ochrony Studentów-kredytobiorców (*Student Borrower Protection Center*; dalej jako: SBPC) opublikowało raport wskazujący, że wykorzystywanie danych związanych z edukacją w procesie uczenia SI może przyczyniać się do po-

⁷⁹ Zob. https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf, dostęp: 27 grudnia 2023 r.

⁸⁰ Zob. K. Langenbucher i P. Corcoran, *Responsible AI Credit Scoring – A Lesson from Upstart.com*, [w:] *Digital Finance in Europe: Law, Regulation, and Governance*, red. E. Avgouleas i H. Marjosola, De Gruyter 2021, s. 141–180, <https://www.degruyter.com/document/doi/10.1515/9783110749472-006/html>, , dostęp: 29 grudnia 2023 r.

⁸¹ Np. FICO credit score.



głębiania nierówności w społeczeństwie⁸². Wniosek ten potwierdzony został przez następujący eksperyment. SBPC przedstawiło studium przypadku, które zbadało wykorzystanie przez Upstart informacji o instytucjach edukacyjnych. Aby przeprowadzić to studium przypadku, SBPC złożyło wiele wniosków za pomocą platformy Upstart. Każdy wniosek został złożony w imieniu 24-letniego mieszkańca Nowego Jorku z tytułem licencjata, ale wnioski o wycenę różniły się między sobą uniwersytetem (lub college'em), który ukończył wnioskodawca, przy jednoczesnym zachowaniu innych danych wejściowych – takich jak historia zatrudnienia, dochód i oszczędności – bez zmian. W raporcie przedstawiono wyniki trzech z tych wniosków, reprezentujących trzy różne instytucje edukacyjne: Uniwersytetu w Nowym Jorku; Uniwersytetu Howard'a⁸³; oraz Uniwersytetu Stanu Nowy Meksyk⁸⁴.

Raport wykazał, że **wysokość oprocentowania i opłat początkowych zaproponowanych przez platformę Upstart różniły się między tymi trzema szkołami, przy czym absolwent NYU płacił o 1724 USD mniej niż absolwent Uniwersytetu Stanu Nowy Meksyk i 3499 USD mniej niż absolwent Uniwersytetu Howard'a**, przez cały okres trwania pożyczki.

Wskutek powyższych obserwacji, Upstart zainicjował prace nad przebudowaniem wykorzystywanego systemu AI tak, aby nie powielał on uprzedzeń rasowych. Proces ten monitorowany jest przez Agencję Ochrony Praw Konsumentów (*Consumer Financial Protection Bureau*), która wystosowała wobec Upstart tzw. „no-action letter”, tj. gwarancję odstąpienia od podejmowania dalszych działań prawnych do czasu wdrożenia określonych przez ww. agencję rozwiązań.

Case study 3

Ochrona prywatności stanowi jedno z najpoważniejszych wyzwań stojących przed twórcami systemów sztucznej inteligencji, a kwestia ta nabiera dodatko-

wego znaczenia w kontekście zastosowań AI w sektorze bankowym. Jak pokazuje przykład OpenAI, twórcy popularnego chatbota ChatGPT, szczególnie istotne ryzyko prawne związane jest z gromadzeniem i wykorzystywaniem danych osobowych⁸⁵ oraz własności intelektualnej⁸⁶ w procesie tworzenia modeli językowych.

New York Times twierdzi, że **modele sztucznej inteligencji stworzone przez OpenAI są zdolne do generowania treści, które w sposób dokładny odwzorowują treść artykułów pojawiających się w gazecie oraz na stronie internetowej, lub ściśle je podsumowują, a także naśladują cechy charakterystyczne dla stylu publicystycznego** wydawanego periodyka. Gazeta twierdzi, że bezprawne wykorzystanie jej pracy do tworzenia modeli AI narusza jej prawa autorskie i dąży do pociągnięcia OpenAI do odpowiedzialności za wyrządzone szkody.

Z kolei strona powodowa w sprawie *A.T. et al v. OpenAI LP et al* zaznacza, że OpenAI i inne spółki bezprawnie pozyskały efekty ich aktywność na platformach mediów społecznościowych i innych witrynach w celu szkolenia swoich systemów sztucznej inteligencji, w tym ChatGPT. Dwóch inżynierów, którzy wnieśli pozew, obawia się, że firmy wykorzystywały ich umiejętności i wiedzę do opracowania narzędzi, które w przyszłości mogą przyczynić się do utraty zatrudnienia przez wielu specjalistów z branży. Inżynierowie zwrócili się do sądu o odszkodowanie w nieokreślonej wysokości oraz o nakazanie pozwanym wdrożenia zabezpieczeń zapobiegających niewłaściwemu przetwarzaniu informacji istniejących w Internecie.

Na dzień oddania raportu powyższe postępowania nie uległy jeszcze zakończeniu, stąd nie można wskazać w jaki sposób sądy podeszły do przedstawionych problemów, ale warto monitorować rozwój wskazanych spraw. Nie budzi jednak wątpliwości, że problemy te istnieją i w toku wdrażania systemów sztucznej inteligencji należy mieć je na uwadze.

Finalnie, warto również zasygnalizować istnienie selektywnych rozwiązań legislacyjnych występujących

82 SBPC, „Educational Redlining”, <https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf>, dostęp: 20 grudnia 2023 r.

83 Uczelnia ta należy do grupy tzw. „historically black colleges and universities”, tj. instytucji edukacyjnych powstałych przed wprowadzeniem ustawy o prawach obywatelskich z 1964 r., na których mogli studiować czarnoskórzy Amerykanie.

84 Uczelnia ta należy do grupy tzw. „hispanic serving institutions”, tj. szkół wyższych, w których przynajmniej 25% studentów stanowią osoby pochodzenia latynoskiego.

85 A.T. et al v. OpenAI LP et al, Case 3:23-cv-04557 (N.D. Cal. Sept. 5, 2023), <https://ipwatchdog.com/wp-content/uploads/2023/10/OPENAI-PRIVACY-LAWSUIT-complaint-1.pdf> (complaint), dostęp: 2 stycznia 2024 r.

86 The New York Times Company v. Microsoft Corporation, Case 1:23-cv-11195 (S.D.N.Y. Dec. 27, 2023), https://nytimes-assets.nytimes.com/2023/12/NYT_Complaint_Dec2023.pdf (complaint), dostęp: 2 stycznia 2024 r.

w prawodawstwie poszczególnych stanów⁸⁷. Dla przykładu, w Teksasie utworzono radę doradczą ds. sztucznej inteligencji, do której zadań należy badanie i monitorowanie systemów sztucznej inteligencji opracowanych, wykorzystywanych lub zamawianych przez agencje stanowe⁸⁸. W Dakocie Północnej z definicji legalnej pojęcia „osoba” wprost wyłącza się sztuczną inteligencję⁸⁹.

Powyższy obraz aktywności pokazuje jak wieloaspektowa, a dzięki temu kompleksowa oraz spójna, może być stymulacja rozwoju AI przez podmioty państwowe w postaci tak podmiotów prawodawczych w sensie ścisłym, jak i regulatorów. Jednocześnie szeroki zakres przewidzianych prac legislacyjnych oraz inicjatyw już podjętych w USA wpływa, i przypuszczalnie będzie oddziaływał w coraz większym stopniu, na międzynarodowy dyskurs o AI.

Ponadto, wyraźne jest kładzenie nacisku nie tylko na wykreowanie otoczenia normatywnego dla procesów tworzenia i stosowania sztucznej inteligencji, ale również ukształtowanie warunków infrastrukturalnych oraz ekonomicznych dla dalszego rozwoju AI.

Doświadczenia USA skłaniają do zaakcentowania **ostrożności z jaką, przynajmniej na obecnym etapie rozwoju sztucznej inteligencji, ustawodawca federalny podchodzi do użycia prawa jako sztywnych ram ograniczających rozwój i wykorzystanie AI**. Obserwować jest bowiem oddziaływanie przede wszystkim za pomocą prawa „miękkiego” (tzw. „soft-law”), a zatem norm nie posiadających bezpośredniej mocy wiążącej. Z powyższego nie można jednak wyprowadzić wniosku, jakoby nieznaczny był zakres ich realnego oddziaływania. Niewiążące wytyczne wyznaczają punkt odniesienia dla dalszej dyskusji nad pożądanym kształtem regulacji prawnej, są przedmiotem

debaty akademickiej oraz mogą wpływać na decyzje strategiczne twórców systemów sztucznej inteligencji. Wydaje się, że dopiero po tym swoistym „okresie przejściowym”, w którym wyłaniane oraz poddawane próbie są różne rozwiązania prawne związane z regulacją AI, przyjdzie w prawodawstwie federalnym USA czas na ustanawianie aktów normatywnych o bardziej stanowczym charakterze. Jak pokazują niektóre akty prawne obowiązujące w poszczególnych stanach – proces ten może nabrać w najbliższych latach rozpędu również na poziomie federalnym.

3.3. UK

Kolejnym państwem z kręgu kultury prawnej „common law” jest Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej. Ze względu na pierwotne członkostwo w Unii Europejskiej (dalej również jako: UE), doświadczenie UK stanowi ciekawy przykład pośredniego oddziaływania prawa unijnego przy jednoczesnym wpływie oryginalnych rozwiązań prawnych. Już na wstępie zaznaczyć trzeba, że trudno jest na obecnym etapie, pomimo istnienia (omówionych poniżej) regulacji prawnych odnoszących się pośrednio do kwestii SI, uznać doświadczenie prawne UK za wyjątkowo rozległe. Prawodawca krajowy, podobnie jak miało to miejsce w przypadku USA, w pierwszej kolejności zdecydował się na opracowanie, i poddanie pod szerszą dyskusję w procedurze konsultacji społecznych, granic wyznaczających ogólny kierunek dalszych prac legislacyjnych nad statusem AI.

Dokumentem określającym ww. politykę jest biała księga pt. „Ustanowienie proinnowacyjnego podejścia do regulacji AI” (*Establishing a pro-innovation approach to AI regulation*)⁹⁰. Scharakteryzowano w nim dwa, potencjalnie sprzeczne ze sobą, zasadnicze cele przyszłej regulacji. **Po pierwsze, istotne jest zapewnienie takiej regulacji, która wspierać będzie innowacyjność. Po drugie, konieczne jest zidentyfikowanie i ograniczenie ryzyka związanego z wykorzystaniem AI**. Podczas gdy zapewnienie sztywnych ram służących ochronie praw podstawowych może przyczynić się do wyhamowania rozwoju sztucznej inteligencji, przyjęcie odmiennej strategii jest równie trudne do zaakceptowania, a to przez wzgląd właśnie na potrzebę ochrony praw człowieka. Postulowana regulacja musi odpowiadać na obie wyżej zidentyfikowane potrzeby. Stąd,

87 Trzeba w tym miejscu odnotować, że przedmiotowy raport – ze względu na rozległość zagadnienia jakim jest prawodawstwo stanowe związane z AI – może jedynie zasygnalizować istnienie pewnych rozwiązań prawnych. Prowadzony jest jednak wykaz ww. prawodawstwa. Zob. <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation>, dostęp: 16 grudnia 2023 r.

88 Zob. *Relating to the creation of the artificial intelligence advisory council Act*, H.B. 2060, 88th Legislature, Regular Session (2023), <https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB2060>, dostęp: 9 stycznia 2024 r.

89 Zob. *To create and enact a new section to chapter 1-08 of the North Dakota Century Code, relating to personhood status; to provide for application; and to declare an emergency Act*, H.B. 1361, N.D. Legis., 67th Sess. (2023), https://ndlegis.gov/assembly/68-2023/regular/bill-overview/bo1361.html?bill_year=2023&bill_number=1361, dostęp: 9 stycznia 2024 r.

90 Zob. <https://assets.publishing.service.gov.uk/media/64cb71a547915a00142a91c4/a-pro-innovation-approach-to-ai-regulation-amended-web-ready.pdf>, dostęp: 5 stycznia 2024 r.

proponuje się opracowanie przepisów, koncentrując uwagę nie tyle na konkretnych rozwiązaniach technologicznych, co na kontekstach, w których wdrażane i wykorzystywane jest AI. Tytułem przykładu wskazano, że to samo narzędzie w dwóch różnych użyciach (podsumowanie artykułu naukowego i udzielenie porady medycznej) może borykać się z odmiennymi trudnościami. To zaś w kontekście ram niniejszego raportu, tj. sektora bankowości, pozwala, a wręcz skłania do wskazania, że w tym zakresie powinno się proponować z jednej strony narzędzia wprost przeznaczone dla banków, z drugiej zaś niektóre narzędzia mogą zostać dostosowane właśnie pod użytek bankowy. Wówczas jednak będzie należało skupić się na istniejących i potencjalnych trudnościach właściwych temu właśnie sektorowi. Stąd już w tym miejscu zaznaczyć należy, że szczególne znaczenie w interesującym nas zakresie może mieć nie tylko prawodawstwo zwykłe, ale również, a może przede wszystkim, działalność regulatorów właściwych dla sektora bankowego, znających jego bolączki, problemy i specyfikę.

Dalej odnotowuje się szczególną pozycję agencji rządowych pełniących funkcję regulatorów w określonych sektorach. W ocenie prawodawcy krajowego znają one potencjalne ryzyka występujące w poszczególnych branżach, a także posiadają kompetencje i wiedzę niezbędne dla zapewnienia proporcjonalnej ingerencji w razie ewentualnych naruszeń związanych z wykorzystaniem AI. W ten sposób agencje te z jednej strony są zdolne do wspierania innowacji oraz ścisłej współpracy z przedsiębiorcami, zaś z drugiej strony mogą skutecznie przeciwdziałać ryzyku, gdy ingerencja staje się konieczna. Proponowana regulacja powinna zatem wspierać agencje w dotychczasowej działalności – zapewniając w tym zakresie niezbędną elastyczności w prowadzeniu działań – przy jednoczesnym dążeniu do zapewnienia względnej spójności w działaniach podejmowanych przez poszczególne agencje. Drugi z wymienionych celów realizowany miałby być na poziomie **administracji rządowej, do której należałoby: monitorowanie ogólnej skuteczności regulacji prawnej w całej gospodarce, prowadzenie analiz pojawiających się trendów technologicznych w zakresie sztucznej inteligencji i koordynowanie odpowiedzi na nie, wspieranie platform testowych i inicjatyw typu sandbox⁹¹, zapewnienie działań po-**

pularyzatorskich oraz promowanie interoperacyjności w granicach przewidzianych przez przepisy prawa międzynarodowego.

Prospektywny charakter wyżej opisanych prac legislacyjnych nie oznacza jednak, że problematyka wykorzystania AI została dotychczas całkowicie pominięta. Jedną z nadrzędnych koncepcji wypracowanych we wskazanej białej księdze jest bowiem wzmocnienie funkcjonujących już w systemie prawnym rozwiązań. Widać zatem wyraźnie, że w zamyśle prawodawcy UK **zmiana normatywna w zakresie stosowania SI nastąpić ma nie poprzez zmianę, czy też dodanie, odpowiednich przepisów, lecz w drodze odpowiedniej ich interpretacji.** Z tego względu konieczne jest zaprezentowanie relewantnych dla sektora bankowego przepisów prawa.

W pierwszej kolejności warto pochylić się nad ustawą o ochronie danych⁹². Jej uchwalenie stanowiło pierwotnie implementację przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)⁹³. Nawet po opuszczeniu UE przez Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej akt ten zachował moc wiążącą, co nie oznacza, że funkcjonuje on obecnie w niezmienionej postaci.

Choć prawdą jest, że UK GDPR w znacznym stopniu powieli regulację znaną z RODO, to występują jednak pomiędzy nimi pewne rozbieżności, które widoczne są w szczególności po zestawieniu UK GDPR z pozostałymi częściami DPA 2018. Do najistotniejszych różnic merytorycznych należą przepisy, które umożliwiają odstępianie od obowiązków przewidzianych w UK GDPR w określonych przypadkach ze względu na konieczność zachowania bezpieczeństwa narodowego – pod warunkiem spełnienia **testów proporcjonalności, konieczności i legalności rzeczonego działania⁹⁴**. Wprowadzie RODO przewiduje zbliżony mechanizm, który pozwala państwom członkowskim na ograniczenie zakresu ochrony

91 Tj. inicjatyw, których celem jest ułatwienie wprowadzania nowych technologii na rynek. Odnotować można, że w Polsce oferowane jest już narzędzie tego typu. Zob. https://www.knf.gov.pl/en/MARKET/Fintech/Virtual_Sandbox, dostęp: 8 stycznia 2024 r.

92 Data Protection Act 2018, c. 12, <https://www.legislation.gov.uk/ukpga/2018/12/contents>, dostęp: 5 stycznia 2024 r. (dalej jako: DPA 2018). Warto zaznaczyć, że implementacja przepisów prawa unijnego zawarta jest w części drugiej wymienionej ustawy (dalej jako: UK GDPR).

93 Dz. U. UE. L. z 2016 r., nr 119, s. 1-88; dalej jako: RODO.

94 Zob. art. 110 i 111 DPA 2018.



danych osobowych, jednak pozostaje on bardziej restrykcyjny przewidując szerszą ochronę oraz dążąc do utrzymania możliwie jednolitego poziomu ochrony danych. Należy zatem dojść do wniosku, że poziom ochrony danych osobowych w UK – pomimo braku obowiązywania w tym państwie RODO – jest, z nielicznymi wyjątkami, zbliżony do standardów przyjętych w państwach członkowskich UE.

Kolejnym kluczowym aktem normatywnym wpływającym na potencjalne sposoby użycia SI w sektorze bankowym jest ustawa o usługach i rynkach finansowych⁹⁵ oraz akty wykonawcze do niej⁹⁶. Wprawdzie wypada mieć na uwadze, że to nie twórcy lub dystrybutorzy systemów sztucznej inteligencji będą najczęściej bezpośrednimi adresatami tych norm, jednak powinni oni mieć na względzie, że na podmiotach sektora bankowego ciążyć mogą, mające znaczenie dla wykorzystania AI, szczególne obowiązki wynikające z prawa powszechnie obowiązującego⁹⁷.

W zakresie zasad wykorzystania AI w sektorze bankowym **działalność FCA obejmuje publikowanie materiałów informacyjnych**⁹⁸, a także członkowie wspomnianego regulatora sektorowego **biorą czynny udział w różnego rodzaju konferencjach oraz innych wydarzeniach promujących dobre praktyki, pożądane rozwiązania oraz wiedzę na temat zalet i zagrożeń AI**⁹⁹.

Jednakże z punktu widzenia niniejszego raportu – ze względu na obrazowanie niespotykanego na szeroką skalę modelu prowadzenia konsultacji społecznych w procesie legislacyjnym, który to model stanowić może źródło inspiracji dla ustawodawcy polskiego – znacznie ważniejsze jest prowadzenie przez FCA, niekiedy we współpracy z innymi podmio-

tami¹⁰⁰, **inicjatyw mających za zadanie zaktywizowanie podmiotów związanych z sektorem bankowym do wzięcia udziału w debacie społecznej poświęconej wykorzystaniu AI**. Narzędziem realizacji tego celu jest chociażby publikacja wspólnego dokumentu Banku Angielskiego i FCA pt. „Discussion Paper – Artificial Intelligence and Machine Learning” (dalej jako: DP 5/22)¹⁰¹ oraz dokumentu pt. „Feedback statement – Artificial Intelligence and Machine Learning” (dalej jako: FS 2/23)¹⁰² stanowiącego podsumowanie odpowiedzi udzielonych przez respondentów na pytania postawione w DP 5/22. Warto przybliżyć treść ww. dokumentów.

W DP 5/22 określono pięć obszarów mogących stanowić wyzwania dla wykorzystania AI w sektorze bankowym. Ze względu na ich uniwersalny charakter oraz potencjalne implikacje dla rodzimego dyskursu, konieczne jest ich scharakteryzowanie.

Po pierwsze, zwrócono uwagę na **konieczność ochrony konsumentów**. Obszar ten dotyczy przede wszystkim mechanizmów ograniczania zjawiska dyskryminacji automatycznej.

Po drugie, **wykorzystanie SI nie może ograniczać konkurencji na rynku usług finansowych**. Systemy sztucznej inteligencji umożliwiać bowiem mogą wykrywanie zmiany cen przez konkurentów i szybką lub nawet automatyczną reakcję na zmiany na rynku. W ten sposób AI potencjalnie mogłoby prowadzić, w sposób zamierzony lub też nie, do utworzenia przez podmioty sektora finansowego stanu rzeczy zbliżonego do zмовы cenowej. Ponadto, jak podkreślono w DP 5/22: „koszty wejścia na rynek (dotyczące zarówno personelu i umiejętności, jak i samych danych oraz technologii) mogłyby zostać

95 Financial Services and Markets Act 2000 c. 8, <https://www.legislation.gov.uk/ukpga/2000/8/contents>, dostęp: 5 stycznia 2024 r.

96 W szczególności mowa tutaj o, określającej zasady prowadzenia działalności regulowanej (która co do zasady licencjonowana i nadzorowana jest przez FCA), Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, <https://www.legislation.gov.uk/uksi/2001/544/contents>, dostęp: 6 stycznia 2024 r.

97 Najistotniejsze spośród nich podsumowane zostały w udostępnianym przez FCA „podręczniku”. Zob. <https://www.handbook.fca.org.uk/handbook>, dostęp: 6 stycznia 2024 r.

98 Przykładowo zob. <https://www.fca.org.uk/insight/ai-transparency-financial-services-why-what-who-and-when>, dostęp: 6 stycznia 2024 r.

99 Zob. <https://www.fca.org.uk/news/speeches/ai-flipping-coin-financial-services>, dostęp: 6 stycznia 2024 r.; <https://www.fca.org.uk/news/speeches/our-emerging-regulatory-approach-big-tech-and-artificial-intelligence>, dostęp: 6 stycznia 2024 r.

100 Niech za przykład posłuży Bank Anglii.

101 Zob. Discussion Paper 5/22 – Artificial Intelligence and Machine Learning, <https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence>, dostęp: 6 stycznia 2024 r. Jedynie na marginesie zaznaczyć trzeba, że forma komunikacji prawodawcy ze społeczeństwem jaką jest tzw. „discussion paper” nie ma w polskiej tradycji legislacyjnej swojego odpowiednika. Próbuąc przybliżyć charakterystykę zasygnalizowanej formy działania można by wskazać, że jest to publikacja, często oparta na badaniach naukowych, która obejmuje tematy istotne dla konstruowania polityki oraz analizuje je w szerszym kontekście. „Discussion paper” precyzuje także obszary, w których zachęca respondentów (a dokumenty te ogłaszane są publicznie, przez co każdy zainteresowany podmiot może wziąć udział w dyskusji) do sprecyzowania stanowiska w sprawie.

102 Zob. Feedback Statement 2/23 – Artificial Intelligence and Machine Learning, <https://www.bankofengland.co.uk/prudential-regulation/publication/2023/october/artificial-intelligence-and-machine-learning>, dostęp: 6 stycznia 2024 r.



podniesione do poziomu, który ograniczyłby wejście na rynek z potencjalnie szkodliwym wpływem na konkurencję”.

Po trzecie, **sektor bankowy, w większym stopniu niż ma to miejsce w innych obszarach gospodarki, wymaga bezpieczeństwa i niezawodności wdrażanych rozwiązań technologicznych**. Jednak sama natura SI sprawia, że możliwa jest samodegradacja modelu¹⁰³. Zjawisko to z czasem może sprawić, że same modele, jak i całe systemy sztucznej inteligencji będą mniej stabilne. Ponadto, stopień złożoności modeli sztucznej inteligencji rośnie, co może prowadzić do braku możliwości ich wyjaśnienia lub interpretacji.

Po czwarte, **na szczególną ochronę zasługują posiadacze polis ubezpieczeniowych**. Ponownie zwrócono uwagę na możliwość dyskryminacji automatycznej, występującej potencjalnie już na etapie zawierania umowy. Co więcej, ryzyko związane z wykorzystaniem AI do szacowania przepływów pieniężnych i obliczania rezerw kapitałowych może skutkować niedokładnymi prognozami finansowymi, co z kolei może wpłynąć na zdolność ubezpieczycieli do wywiązania się z przyszłych zobowiązań.

Wreszcie ostatnim z odnotowywanych wyzwań jest **zapewnienie stabilności finansowej i integralności rynku**. Jak zaznaczono, korzystanie z podobnych zestawów danych i algorytmów SI może skutkować ujednoliceniem modeli i podejść w wielu firmach, co może wzmacniać zachowania procykliczne w niektórych przypadkach użycia, takich jak handel algorytmiczny. Rynki mogą również potencjalnie stać się podatne na manipulacje. Dodatkowo uzależnienie podmiotów sektora finansowego od podmiotów zewnętrznych może prowadzić do sytuacji, w której cyberatak na podmiot zewnętrzny wpłynąłby na funkcjonowanie potencjalnie większej liczby podmiotów sektora bankowego.

Warto w tym miejscu przyjrzeć się odpowiedziom respondentów zawartym w FS 2/23. Co może wydawać się zaskakujące, zdaniem respondentów **definicja legalna próbująca określić najszerszy nawet katalog cech sztucznej inteligencji nie byłaby przydatna**. Wskazano na możliwość zastosowania alternatywnych, opartych na zasadach funkcjonowania AI lub ryzyku wykorzystania SI, koncentrując

się na konkretnych cechach sztucznej inteligencji, albo zagrożeniach stwarzanych lub wzmacnianych przez wykorzystanie sztucznej inteligencji. Ze względu na stały postęp w branży AI, zalecono **regularne aktualizowanie wytycznych sektorowych wydawanych przez regulatorów krajowych**. Potencjalne regulacje i dalszy nadzór powinny koncentrować się przede wszystkim na rezultatach wykorzystania AI. Podsumowując FS 2/23 respondenci zauważyli, że obecnie obowiązujące regulacje prawne są w znacznym zakresie wystarczające, aby sprostać zagrożeniom związanym ze sztuczną inteligencją.

Opisana powyżej działalność FCA, jak zostało wcześniej zaznaczone, wpisuje się w kontekst wykorzystywania na szeroką skalę mechanizmów konsultacji społecznych. Przeprowadzona analiza pozwala na przyjęcie, że **do cech charakterystycznych przyjętego w UK modelu stanowienia prawa sztucznej inteligencji należy właśnie daleko idąca zachowawczość w tworzeniu nowych przepisów**. Prymalną metodą regulacji wykorzystania AI jest odpowiednie, tj. uwzględniające kontekst ewentualnych sposobów użycia SI w danym sektorze, stosowanie przepisów już obowiązujących. Zgodnie z nkreśloną w ww. białej księdze strategią legislacyjną, **ustanawianie nowych przepisów, o ile okaże się konieczne, realizowane będzie w obrębie konkretnego wycinka życia społecznego**. W tym zakresie podejście UK nie odnajduje odpowiednika wśród innych porównywanych w niniejszej części raportu państw. Wobec powyższych cech, a także uwzględniając szeroki zakres działań podejmowanych przez FCA, nie powinien zatem dziwić fakt, że regulator ten nie prowadzi aktualnie postępowań w przedmiocie nałożenia sankcji administracyjnych z tytułu niewłaściwego wykorzystania AI.

3.4. Francja

Kierując uwagę na kontekst doświadczeń innych państw członkowskich Unii Europejskiej, warto rozpocząć od przykładu Francji, stanowiącej reprezentatywny przykład reżimu prawnego właściwego państwu o tradycji romanistycznej (czyli relatywnie bliskiego polskiej tradycji prawnej). Państwo to wyraziło przede wszystkim chęć podjęcia współpracy nad regulacją AI na arenie międzynarodowej, określając USA jako kluczowego partnera w tym zakresie¹⁰⁴.

¹⁰³ Szerzej zob. F. Bayram, B.S. Ahmed, i A. Kassler, *From concept drift to model degradation: An overview on performance-aware drift detectors*, „Knowledge-Based Systems”, 245/2022.

¹⁰⁴ Zob. <https://www.cnbc.com/2023/06/15/ai-regulation-france-sees-ideas-on-global-laws-by-end-of-year.html>, dostęp: 17 grudnia 2023 r.

Ponadto, dostrzegane są potencjalne korzyści płynące ze wzmożenia aktywności naukowej w sektorze AI. Cel ten ma być osiągnięty za pomocą wdrażania **rozmaitych polityk publicznych z Krajową strategią na rzecz sztucznej inteligencji** (*Stratégie nationale pour l'intelligence artificielle*) na czele¹⁰⁵. Planowane jest między innymi przeznaczenie, w ramach programu Interdyscyplinarne instytuty sztucznej inteligencji (*Instituts Interdisciplinaires en IA*), **znacznych środków finansowych mających przyczynić się do stworzenia optymalnych warunków dla dalszych badań nad technologią SI**¹⁰⁶. Przede wszystkim nacisk położony został na zgromadzenie wybitnych naukowców poprzez działalność grantodawczą. Program ten koncentruje się na **organizowaniu interdyscyplinarnych badań i współpracy z przemysłem**. Dzięki finansowaniu w wysokości 75 mln euro w ramach trzeciego komponentu programu Inwestycje w Przyszłość (*Le Programme d'Investissements d'Avenir*), powołane instytuty otrzymają również wsparcie finansowe zarówno od partnerów publicznych, jak i prywatnych. Łącznie na projekty badawcze prowadzone w instytutach wydanych zostanie 225 mln euro.

Aktywność Francji nie ogranicza się wyłącznie do wystosowywania deklaracji o charakterze politycznym, czy też wspierania rozwoju naukowego. Warto odnotować, że istotnym kontekstem dla regulacji krajowej wszystkich państw członkowskich Unii Europejskiej jest RODO. Wspomniany akt normatywny, a także inne relewantne inicjatywy prawodawcze podejmowane przez Unię Europejską, staną się przedmiotem szczegółowej analizy w kolejnym rozdziale niniejszego raportu. Stąd, w tym miejscu jedynie zasygnalizować można związek prawodawstw krajów członkowskich UE z unijnymi regulacjami prawnymi¹⁰⁷.

Oprócz przepisów realizujących obowiązki wynikające z RODO istotną rolę odegrało także uchwalenie ustawy z dnia 7 października 2016 r. O Republice Cyfrowej¹⁰⁸. Ze względu na ramowy charakter przytoczonej regulacji warto chociaż pokrótce ją przybli-

żyć. Do zasadniczych celów omawianej ustawy należy kształtowanie bezpiecznej przestrzeni cyfrowej, w której mogliby poruszać się obywatele. Materię stanowiącą przedmiot ww. aktu normatywnego podzielić można na trzy zasadnicze obszary. Pierwsza grupa zagadnień dotyczy dostępu do rynku usług cyfrowych oraz neutralności przestrzeni cyfrowej. Druga grupa zagadnień obejmuje tematykę funkcjonowania gospodarki opartej na wykorzystaniu danych utrwalonych w formie elektronicznej. Jest to, w ocenie ustawodawcy francuskiego, szybko rozwijający się sektor, który ma ogromny potencjał, aby przyczynić się zarówno do wzrostu gospodarczego, jak i rozwoju społecznego. Trzeci, i ostatni zarazem, rozdział ustawy porusza kwestię dostępu do usług cyfrowych w ramach funkcjonowania rynku usług cyfrowych.

W pewnym zakresie powyższa regulacja wpływać będzie na wykorzystanie systemów sztucznej inteligencji wprost. Zgodnie z art. 4 ww. Aktu normatywnego, w kodeksie relacji między społeczeństwem a administracją (*Code des relations entre le public et l'administration*)¹⁰⁹ dodano art. L.311-3-1, w myśl którego **indywidualna decyzja podjęta na podstawie przetwarzania algorytmicznego zawiera wyraźne oświadczenie informujące o tym fakcie stronę postępowania. Dodatkowe informacje wykorzystania przetwarzania algorytmicznego udzielane są na wniosek strony postępowania**. Zgodnie z art. R.311-3-1-1 wspomnianego kodeksu, oświadczenie, o którym mowa w art. L.311-3-1: wskazuje cel przetwarzania algorytmicznego; poucza o prawie do uzyskania informacji, o zasadach określających przetwarzanie algorytmiczne, a także o procedurach korzystania z tego prawa; poucza o możliwości skierowania skargi do komisji ds. dostępu do dokumentów administracyjnych. Z kolei na podstawie art. R.311-3-1-2, organ administracji przekazuje osobie, której dotyczy indywidualna decyzja podjęta na podstawie przetwarzania algorytmicznego, na jej wniosek, w zrozumiałej formie i z zastrzeżeniem nienaruszania tajemnic prawnie chronionych, informacje dotyczące: 1) stopnia i sposobu, w jaki przetwarzanie algorytmiczne przyczyniło się do podjęcia decyzji o określonej treści; 2) przetwarzania danych i ich źródła; 3) parametrów podlegających przetworzeniu i, w stosownych przypadkach, ich znaczenia, dla kie-

¹⁰⁵ Zob. <https://www.economie.gouv.fr/strategie-nationale-intelligence-artificielle#>, dostęp: 4 stycznia 2024 r.

¹⁰⁶ Zob. <https://www.investincotedazur.com/en/ai-cluster-and-ai-booster-france-2030-the-pillars-of-french-strategy-in-ai/>, dostęp: 4 stycznia 2024 r.

¹⁰⁷ Co oczywiste, uwaga ta zachowuje swoją ważność również w odniesieniu do sytuacji prawnej Niemiec.

¹⁰⁸ LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique, nr NOR: ECFI1524250L, JORF n° 0235 du 8 octobre 2016.

¹⁰⁹ https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000031366350?init=true&page=1&query=Code+des+relations+entre+le+public+et+l%27administration&searchField=ALL&tab_selection=all, dostęp: 2 stycznia 2024 r.



runku rozstrzygnięcia sprawy; 4) operacji wykonywanych w ramach przetwarzania algorytmicznego.

Choć **przytoczona regulacja kreuje wyłącznie obowiązki po stronie organów administracji, to sformułowane w niej zalecenia stanowią źródło inspiracji dla dalszych wytycznych CNIL, a zatem przynajmniej pośrednio oddziałują również na podmioty sektora prywatnego.**

Nakierowując uwagę na aktualnie procedowane inicjatywy ustawodawcze warto odnotować przedłożenie Zgromadzeniu Narodowemu projektu ustawy w przedmiocie ram dla sztucznej inteligencji wynikających z prawa autorskiego (*proposition de loi visant à encadrer l'intelligence artificielle par le droit d'auteur*)¹¹⁰. Projekt przewiduje **wymóg uzyskania zgody autora na wykorzystanie jego utworu przez AI** – zarówno w fazie rozwoju, jak i operacyjnej. Następnie, postuluje się wprowadzenie zbiorowego zarządzania prawami autorskimi do utworów wygenerowanych przez SI. W ocenie projektodawców, prawa te, w odniesieniu do utworów generowanych „w całości”, tj. bez bezpośredniej ingerencji człowieka, prawa autorskie powinny przysługiwać autorom utworów, które wykorzystane zostały w procesie powstawania systemu sztucznej inteligencji. Istotne znaczenie odgrywa również **informowanie użytkowników o źródle wygenerowanego utworu**. Po pierwsze, na wygenerowanym przez system sztucznej inteligencji utworze, konieczne jest umieszczenie słów: „utwór wygenerowany przez AI”. Po drugie, konieczne jest również wyraźne wskazanie nazwisk autorów utworów, które przyczyniły się do wygenerowania konkretnej treści przez AI.

Choć proponowana regulacja nie odnosi się wprost do wykorzystania SI w sektorze bankowym, to jednak na jej podstawie zrekonstruować można zasadnicze motywy przyświecające dotychczasowym przedsięwzięciom ustawodawczym. Wyraźnie zarysowuje się **dążenie do wyważenia dwóch wartości jakimi jest rozwój AI oraz zapewnienie poszanowania dla praw człowieka oraz innych praw podmiotowych jednostek**. Istotną rolę odgrywa obowiązek informacyjny, obejmujący swoim zakresem nie tylko wskazanie na wykorzystanie AI w indywidualnym przypadku, ale również objaśnienie sposobu w jaki dany system sztucznej inteligencji funkcjonuje oraz na podstawie jakich danych wejściowych wygenerował konkretną treść.

Pierwotnie wspomniany CNIL, stanowiący odpowiednik polskiego Urzędu Ochrony Danych Osobowych, powołany został w celu podnoszenia świadomości i dzielenia się informacjami na temat ochrony danych osobowych. Obecnie CNIL ma również uprawnienia doradcze¹¹¹ oraz dochodzeniowe. W ramach swojej działalności wspomniany organ opublikował szereg dokumentów, przybierających najczęściej formę zbioru wytycznych lub tzw. „check-list”, dotyczących zapewniania zgodności wdrażanych rozwiązań technologicznych z RODO oraz innymi aktami normatywnymi stawiającymi określone wymagania dla wykorzystania danych osobowych.

Przykładem powyższej aktywności jest opublikowanie w dniu 21 września 2022 r. przewodnika podsumowującego kluczowe cechy, które posiadać musi system sztucznej inteligencji w świetle regulacji RODO¹¹². Oprócz przytoczenia właściwości istotnych z punktu widzenia każdego procesu przetwarzania danych¹¹³, a opisanych w dalszej części niniejszego raportu, dokument ten omawia ryzyka związane bezdyskusyjnie z wdrażaniem SI. Wymienia bowiem m.in. postulat **istnienia mechanizmów kontroli decyzji wydanych na podstawie przetwarzania algorytmicznego, warunki zgodnego z prawem tworzenia baz danych zawierających dane osobowe wykorzystywane następnie do trenowania systemu sztucznej inteligencji, wymóg nadzoru nad funkcjonowaniem AI w fazie rozwoju oraz w fazie operacyjnej, obowiązek zapobiegania dyskryminacji automatycznej**. Powyższe opracowanie jest tym cenniejsze, że odnosi się do przykładów dobrych praktyk ustalonych na podstawie kontroli przeprowadzonych przez CNIL. Dokument posłużył także do stworzenia check-listy ułatwiającej samodzielną ocenę zgodności projektowanego systemu z RODO¹¹⁴.

Nie można zapomnieć, że CNIL posiada także kompetencję do nakładania sankcji administracyjnych w przypadku stwierdzenia naruszenia zasad wyni-

110 Zob. https://www.assemblee-nationale.fr/dyn/16/textes/l16b1630_proposition-loi, dostęp: 3 stycznia 2024 r.

111 Warto wspomnieć chociażby o tym, że CNIL opiniował m.in. projekt Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii. Zob. <https://www.cnil.fr/en/artificial-intelligence-opinion-cnil-and-its-counterparts-future-european-regulation>, dostęp: 2 stycznia 2024 r.

112 <https://www.cnil.fr/en/ai-ensuring-gdpr-compliance>, dostęp: 2 stycznia 2024 r.

113 Mowa tutaj m.in. o gwarancjach wynikających z art. 9, 11, 15, 16 i 22 RODO.

114 Zob. <https://www.cnil.fr/en/self-assessment-guide-artificial-intelligence-ai-systems>, dostęp: 2 stycznia 2024 r.



kających z krajowych i międzynarodowych regulacji dotyczących ochrony danych osobowych.

Często omawianym w literaturze przedmiotu naruszeniem prawa do ochrony przed dyskryminacją automatyczną jest wykorzystanie niektórych systemów sztucznej inteligencji w działaniach prewencyjnych służb mundurowych. **Modele wykorzystujące dotychczas zebrane dane, pomimo nie posługiwania się wprost kryterium rasy, odtwarzały uprzedzenia rasowe, np. zalecając częstsze patrolowanie obszarów zamieszkiwanych przez mniejszości etniczne**¹¹⁵.

Jak pokazuje praktyka, naruszenia związane z wykorzystaniem AI w kontekście działalności organów ścigania również mieszczą się w obrębie zainteresowań CNIL. Przykładu dostarcza postępowanie zakończone decyzją z dnia 17 października 2022 r. w sprawie Clearview AI¹¹⁶. Oprogramowanie stworzone przez stronę postępowania działa w następujący sposób. W pierwszej kolejności zbierane są wszystkie, dostępne w momencie gromadzenia, obrazy zawierające zdjęcia ludzkich twarzy. Wykorzystywane są w tym celu media społecznościowe oraz inne publicznie dostępne źródła. W ten sposób firma zebrała do chwili zakończenia postępowania ponad dziesięć miliardów zdjęć.

Na podstawie każdego zebranego zdjęcia tworzony jest szablon biometryczny. W ten sposób generowany jest unikalny, ustalany na podstawie analizy punktów twarzy, zestaw cech specyficzny dla oblicza osoby, która pojawia się na zdjęciu. Obrazy, wraz z odpowiadającymi im szablonami biometrycznymi, są następnie zapisywane w bazie danych.

Clearview AI sprzedaje dostęp do platformy internetowej z wyszukiwarką. Narzędzie to jest używane poprzez przesłanie zdjęcia twarzy. Następnie ustalane są cechy specyficzne twarzy widocznej na załączonym zdjęciu i przeprowadzana jest kwerenda w bazie danych zdjęć przejawiających podobne cechy specyficzne. Oprogramowanie generuje wy-

nik, składający się ze zdjęć osób uznanych za podobnych, a także adresów URL stron internetowych, z których zostały pobrane.

Ze względu na brak uzyskania zgody osób, których dane dotyczą, na gromadzenie i wykorzystywanie ich wizerunków oraz niemożność oparcia się na podstawie prawnej uzasadnionego interesu – w świetle inwazyjnego charakteru gromadzenia danych i braku świadomości ze strony obywateli Francji, których dane m.in. dotyczą, na temat gromadzenia danych – w ocenie CNIL, doszło do przetwarzania danych wrażliwych bez podstawy prawnej. To z kolei uzasadniało nałożenie na Clearview AI kary w wysokości 20 mln euro.

Podsumowując doświadczenia Francji wskazać trzeba, co następuje. Po pierwsze, widoczne jest **dążenie do zapewnienia jak najszerzej ochrony prywatności obywateli**. Realizacji tak zakreślonego celu służy w pierwszej kolejności **wprowadzenie licznych obowiązków związanych z informowaniem obywateli o wykorzystaniu i zasadach funkcjonowania AI w konkretnych kontekstach, a także rygorystyczne przestrzeganie przepisów RODO**, co w istotny sposób ogranicza bazy danych, z których z uwagi na niezgodne z RODO przetwarzanie danych osobowych, systemy AI mogą korzystać. Również działalność CNIL w większym stopniu niż, przykładowo, NIST oscyluje wobec zagadnień związanych z ochroną danych. Stanowi to oczywiście następstwo pozycji ustrojowej i zadań stawianych przed tą agencją rządową. Tym niemniej sam fakt, że krajowy regulator AI czuwa jednocześnie nad przestrzeganiem przepisów prawa ochrony danych osobowych podkreśla ścisły związek między tymi zagadnieniami we francuskim systemie prawa. Po drugie, **ustawodawca francuski w wyższym stopniu niż ma to miejsce w pozostałych badanych porządkach prawnych, już na tym etapie rozwoju legislacji dotyczącej AI, tworzy prawo posiadające określoną moc wiążącą, w tym restrykcyjne przepisy będące źródłem konkretnych i precyzyjnych norm prawnych**. Instrumenty o charakterze miękkim, jak np. wytyczne CNIL, pełnią jedynie funkcję pomocniczą. Przypuszczalnie opisany stan rzeczy związany jest z pierwszą podkreśloną właściwością doświadczenia legislacyjnego Francji. Narzędziem właściwym do ustanawiania mechanizmów ochrony fundamentalnych praw człowieka jest bowiem ustawa, której przestrzeganie gwarantowane jest między innymi na drodze postępowania administracyjnego. Po trzecie, **Francja dostrzega związek rozwoju technologicznego w zakresie AI z nauką – stąd wspiera-**

¹¹⁵ Szerzej zob. K. Lum i W. Isaac, *To Predict and Serve?*, „Significance”, 5(13)/2016, s. 14-19; T.-W. Hung i C.-P. Yen, *Predictive policing and algorithmic fairness*, „Synthese”, 6(201)/2023, s. 4-6. Warto zatem zauważyć, że system sztucznej inteligencji doprowadził tu do podobnego w istocie skutku dyskryminującego, co omówiony wcześniej system dla przygotowania oferty kredytowej firmy Upstart.

¹¹⁶ Délibération de la formation restreinte n° SAN-2022-019, <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046444859?isSuggest=true>, dostęp: 4 stycznia 2024 r.

nie aktywności badawczej, aktywność interdyscyplinarnych grup naukowców oraz ich finansowanie poprzez granty państwowe. Beneficjentem wzmożonej aktywności naukowej będzie również sfera finansowa, a zatem również bankowa, która wskazywana jest niekiedy jako jeden z głównych obszarów wykorzystania AI¹¹⁷.

3.5. Niemcy

Kontynuując rozważania dotyczące obszaru europejskiego – w tym krajów o zbliżonej do polskiej tradycji prawnej, stanowiących w przeszłości wzór lub przynajmniej punkt wyjścia dla rozwiązań krajowych – warto zwrócić uwagę na kolejne państwo, które w unijnym środowisku wyznacza niekiedy pewnego rodzaju trendy legislacyjne. W obszarze uregulowania problematyki sztucznej inteligencji oraz jej narzędzi Niemcy nie mają jednak, jak dotąd, znacznych osiągnięć. Stan ten może oznaczać, że jako państwo członkowskie UE, mając na względzie plany prawodawcy unijnego, stwierdzono, iż **w pierwszej kolejności warto poczekać na to, jakie regulacje zostaną przyjęte na tym poziomie (ponadnarodowym), a dopiero później w prawie wewnętrznym uregulować, czy też doregulować te kwestie, które tak z perspektywy prawnej, jak i aktywnej będą tego wymagały.**

Aby jednak nie pozostać w tyle w zakresie bezsprzecznego rozwoju i ingerowania w coraz to większą liczbę sfer życia codziennego przez sztuczną inteligencję **na poziomie rządowym postanowiono o przyjęciu pewnych regulacji o charakterze miękkim.** W tym zakresie sporządzona została Narodowa strategia rządu federalnego dotycząca sztucznej inteligencji (*Die Nationale Strategie Künstliche Intelligenz der Bundesregierung*)¹¹⁸. Wskazany dokument, porównując go w szczególności z podobnymi założeniami innych omawianych porządków prawnych, ma charakter bardzo ogólny. Zakreśla jednak cele stawiane przed potencjalną regulacją krajową oraz przedstawia plan działań mogących służyć realizacji następujących celów. Po pierwsze, **zwiększona ma zostać konkurencyjność Niemiec na rynku AI.** Po drugie, **gwarantowany ma być**

odpowiedzialny rozwój omawianej technologii. Po trzecie, **uwzględnione muszą zostać implikacje prawne, kulturowe, etyczne i społeczne coraz szerszego wykorzystania SI.** Taki dokument z całą pewnością pozwala na podejmowanie działań zmierzających do praktycznego wdrożenia i rozwoju AI. Nie daje on jednak możliwości wskazania lub choćby przewidzenia precyzyjnych ram prawnych, których w tym zakresie będzie chciał trzymać się niemiecki prawodawca.

W Niemczech zaobserwować można jednak inną, o charakterze nieprawodawczym, działalność związaną z próbą poradzenia sobie z wyzwaniami związanymi z pojawianiem się i rozwojem systemów sztucznej inteligencji w świecie finansowym. Mowa tu o **opracowaniach niemieckiego organu nadzoru nad rynkiem finansowym (BaFin, niem. Bundesanstalt für Finanzdienstleistungsaufsicht).** Instytucja ta chociaż nie tworzy w ten sposób norm o charakterze prawnym, to jednak wskazuje na pewne zasady i stara się wykształcić dobrą praktykę przykładowo w zakresie stosowania sztucznej inteligencji w obszarze podejmowania decyzji¹¹⁹. **Normy te docelowo mogą stać się jednak normami prawnymi, a już dziś można chociażby wstępnie założyć, że będą one stanowiły przynajmniej w pewnym zakresie użyteczną wskazówkę dla niemieckiego prawodawcy.**

Wyraźny jest również wpływ związków zawodowych na dyskurs dotyczący wykorzystania AI¹²⁰. Szczególnym przejawem tejże aktywności jest **działalność Federacji Niemieckich Związków Zawodowych (Deutscher Gewerkschaftsbund; dalej jako: DGB)**¹²¹. Co warto odnotować, niemieckie związki zawodowe nie akcentują obawy przed utratą miejsc pracy. Choć możliwy wydaje się scenariusz, w którym ludzka praca zastępowana jest przez zautomatyzowane procesy nadzorowane przez SI, to jednak skala wdrażania takich rozwiązań nie jest na obecnym etapie

117 Zob. S. Benhamou, *Artificial Intelligence and the Future of Work*, „Revue d'économie industrielle”, 169/2020, s. 58.

118 Zob. https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/201201_Fortschreibung_KI-Strategie.pdf&cid=947, dostęp: 8 stycznia 2024 r.

119 Zob. przykładowo https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_Prinzipienpapier_BDAI_en.html?nn=9866146, dostęp: 1 stycznia 2024 r.; https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2023/fa_bj_2305_Algorithmen_Kreditvergabe_en.html, dostęp: 8 stycznia 2024 r.

120 Szerzej zob. M. Krzywdzinski, D. Gerst, i F. Butollo, *Promoting human-centred AI in the workplace. Trade unions and their strategies for regulating the use of AI in Germany*, „Transfer: European Review of Labour and Research”, 1(29)/2023, s. 53-70.

121 Zob. DGB, *Artificial Intelligence (AI) for Good Work*, 2020, <https://www.dgb.de/++co++b7f96674-9f2e-11ea-a8e8-52540088cada/Concept-Paper-Artificial-Intelligence-AI-for-Good-Work.pdf>, dostęp: 9 stycznia 2024 r.



uznawana za wymagającą stanowczej ingerencji¹²². Dostrzega się ryzyko polegające na **konieczności zapewnienia stałego dokształcania pracowników w zakresie obsługi narzędzi wykorzystujących AI**. Podkreśla się także wątek nieprawidłowego przetwarzania danych osobowych przez AI, które mogą naruszać zasady ochrony prywatności pracowników i potencjalnie umożliwiać ich inwigilację. Nie zapomina się również o **problematyce dyskryminacji automatycznej**. Zdaniem DGB wszystkie sygnalizowane ryzyka mogą jednak zostać zażegnane, pod warunkiem racjonalnego uregulowania sposobów użycia AI¹²³.

Postawę Niemiec w zakresie regulacji AI określić można jako zachowawczą. Ma to związek z prowadzonymi na forum UE pracami legislacyjnymi, które wyznaczają wiążąco kierunek projektowanych norm prawnych. Warto jednak odnotować, że tematyka wykorzystania AI, przynajmniej pośrednio, regulowana jest obowiązującymi aktami prawa unijnego, w tym np. RODO. W dalszej kolejności szczególnie widoczna jest aktywność związków zawodowych, które wskazują na niektóre zagrożenia związane z wykorzystaniem SI, proponując przy tym pewne sposoby ich ograniczenia. Dopiero wejście w życie aktów normatywnych prawa unijnego pozwoli na określenie w jakim zakresie postulaty związków zawodowych zostaną w praktyce legislacyjnej spełnione.

3.6. Chiny

Odmienne niż w państwach europejskich, jak również w USA, w Chinach regulacje prawne poświęcone zagadnieniom związanym z problematyką sztucznej inteligencji nie są nowością, lecz zaczęły pojawiać się już kilka lat temu. W lipcu 2017 r. chińska Rada Stanu wydała krajową strategię rozwoju sztucznej inteligencji. Wskazano tam, że **strategia ta pozwolić ma Chinom na osiągnięcie celu jakim jest stanie się światowym liderem w obszarze sztucznej inteligencji do 2030 r.** Już jednak wcześniej, gdyż w 2013 r., w Chinach wydawane i publikowane były dokumenty, z których wynikało, że **jednym z głównych, wręcz krytycznych celów rozwojowych państwa chińskiego jest właśnie działalność i rozwój sztucznej inteligencji w różnych dziedzinach**

życia¹²⁴. We wskazanych dokumentach zwracano uwagę nie tylko na potrzebę rozwoju AI, ale również na to, że powinno odbywać się to z zachowaniem właściwych standardów i norm etycznych. Chiny stwierdziły również, że od 2017 do 2030 r. planują wydać na rozwój infrastruktury potrzebnej do rozwoju sztucznej inteligencji 150 mld jenów, co odpowiada około 21 mld dolarów. Do 2025 r. **planowany jest wzrost wartości aktualnej infrastruktury w tym zakresie do ponad 400 mld juanów, co odpowiada około 58 mld dolarów**, stworzenie dalszych planów rozwojowych, jak i skodyfikowanie problematyki AI wraz z ustanowieniem jednoznacznych standardów etycznych w tym zakresie.

Plany rozwojowe zaprojektowane przez Chiny koordynowane mają być na szczeblu rządowym przez Ministerstwo Nauki i Technologii, Biuro ds. Promocji Planów Sztucznej Inteligencji, jak również inne istotne z tego punktu widzenia podmioty. Nie oznacza to jednak, że rozwój ten następować ma jedynie na szczeblu centralnym. Państwo środka przewidziało również programy, których celem jest zmotywowanie także podmiotów prywatnych do prowadzenia badań i rozwijania problematyki sztucznej inteligencji¹²⁵. Dotychczasowe doświadczenia wskazują, że programy te spełniają swoją rolę i poszczególne podmioty prywatne rozwijają technologię związaną ze sztuczną inteligencją, a mającą mieć zastosowanie w służbie publicznej. Doskonałymi przykładami są tu firmy Baidu (narodowy mistrz AI w zakresie rozwoju autonomicznych pojazdów), Alibaba (narodowy mistrz AI w zakresie rozwijania sfery inteligentnych miast) oraz Tencent (narodowy mistrz AI w zakresie „wizji komputerowej” dla diagnoz medycznych)¹²⁶. Co interesujące, również w zakresie zadań związanych z sądownictwem wdrażane są podobne programy. Propagowana jest wręcz idea „smart-sądów”. W ramach tego pomysłu sztuczną inteligencję planuje się wykorzystać w obszarze gromadzenia dowodów, analizy spraw oraz lektury

122 M. Krzywdzinski, D. Gerst, i F. Butollo, *Promoting human-centred AI...*, s. 61.

123 DGB, *Artificial Intelligence (AI) for Good Work*, s. 11.

124 H. Roberts, J. Cows, J. Morley, M. Taddeo, V. Wang, L. Floridi, *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*, „AI & Society”, 36/2021, s. 60.

125 H. Roberts, J. Cows, J. Morley, M. Taddeo, V. Wang, L. Floridi, *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*, „AI & Society”, 36/2021, s. 61.

126 Jing M, Dai S (2017) *China recruits Baidu, Alibaba and Tencent to AI 'national team'*. South China Morning Post, <https://www.scmp.com/tech/china-tech/article/2120913/china-recruits-baidu-alibaba-and-tencent-ai-national-team>, dostęp: 18 grudnia 2023 r.

dokumentów prawnych¹²⁷. Analogicznie można byłoby sobie wyobrazić sytuację, w ramach której państwo zorganizowało by konkurs na najlepsze oprogramowanie sztucznej inteligencji w służbie bankowości. Oczywiście inicjatywa taka dotyczyłaby zapewne w głównej mierze bankowości centralnej, z uwagi na to, że to właśnie w szczególności ona znajduje się w zainteresowaniu państwa na tyle, aby narzędzie służące jej rozwojowi chciało tworzyć państwo. Sam sektor bankowy mógłby jednak jako taki również poprowadzić lub skoordynować wspólne badania rozwojowe, które motywowałyby firmy technologiczne do tego, aby stworzyć jak najlepsze narzędzia AI do wykorzystania w bankowości.

Państwo Środka nie poprzestaje jednak na aktach prawa miękkiego, jak również jedynie na zapowiedziach związanych z rozwojem wykorzystania sztucznej inteligencji. Na uwagę zasługują wydawane kolejno przepisy prawa poświęcone tej problematyce. I tak w szczególności uwagę zwracają akty prawne wydane w 2023 r., jako będące tymi o charakterze zdecydowanie najświeższym. Mowa tu o: rozporządzeniu w sprawie generatywnej sztucznej inteligencji oraz przepisach poświęconych ocenie strony etycznej działalności podejmowanej z AI.

Przechodząc do szczegółów, wskazać należy, że w kwietniu 2023 r. chińskie Ministerstwo Nauki i Technologii opublikowało projekt aktu prawnego dotyczącego **środków służących ocenie etycznej działalności podejmowanej z AI**. W dokumencie tym skoncentrowano się przede wszystkim na przeglądzie etycznym działań naukowych i technologicznych, które niosą za sobą największe ryzyka etyczne, w tym w szczególności przy prowadzeniu badań i działalności rozwój¹²⁸.

Z kolei w lipcu 2023 r. Administracja Cyberprzestrzeni Chin, Krajowa Komisja Rozwoju i Reform, Ministerstwo Edukacji, Ministerstwo Nauki i Technologii, Ministerstwo Przemysłu i Informatyki Technologicznej oraz Ministerstwo Bezpieczeństwa Publicznego wspólnie wydały **rozporządzenie w sprawie generatywnej sztucznej inteligencji**. Celem tego aktu było

szerokie uregulowanie problemu generatywnej AI. Co jednak interesujące, **już w momencie wydania rozporządzenia towarzyszył mu objaśniający komunikat wraz z pytaniami i odpowiedziami dotyczącymi należytego sposobu rozumienia wydanych przepisów**¹²⁹.

Rozważając problematykę regulacji prawnych poświęconych przedmiotowym zagadnieniom nie sposób nie wspomnieć o pierwszym rozporządzeniu o charakterze ogólnym, obowiązującym zatem w całych Chinach, które weszło w życie wraz z początkiem marca 2022 r. Rozporządzenie to reguluje wykorzystanie technologii rekomendacji algorytmów do świadczenia usług online w Państwie Środka¹³⁰.

Obecnie obowiązujące regulacje prawne pozwalają odtworzyć jedynie pewną część obrazu, w którym uczestniczą Chiny biorące udział w jednym z najnowszych wyścigów technologicznych. Analitycy chińskiej działalności legislacyjnej wskazują, że regulacja zagadnień związanych ze sztuczną inteligencją może podzielić los regulacji związanych z problematyką Internetu, z tym, że w tym przypadku działania podejmowane przez chińskiego prawodawcę mogą okazać się znacznie szybsze. O ile w pierwszym okresie swoistą cezurą była wydana w 2017 r. ustawa o cyberbezpieczeństwie, o tyle kompleksowa ustawa o AI spodziewana jest jeszcze w tym roku¹³¹. Co więcej projekt takiej ustawy, jako efekt prac naukowców ujrzał światło dzienne już w sierpniu ubiegłego roku¹³². Rozdział pierwszy reguluje problematykę ogólną, w tym najistotniejsze i najbardziej podstawowe zasady prawne. Następnie zajęto się kwestią wsparcia rozwoju i promocji AI. W trzecim rozdziale położono nacisk na kwestie zarządzania systemami sztucznej inteligencji. Czwarty rozdział poświęcono z kolei obowiązkowi, które ciążą mają na osobach odpowiedzialnych za rozwój systemów AI, ich twórców oraz deweloperów. Kolejny rozdział poświęcono problematyce kompleksowego mechanizmu zarządzania sztuczną inteligencją. Zaś ostatni rozdział merytoryczny dotyczy kwestii prawnej odpowiedzialności za działanie i konsekwencje spowodowane przez systemy AI.

127 H. Roberts, J. Cows, J. Morley, M. Taddeo, V. Wang, L. Floridi, *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*, „AI & Society”, 36/2021, s. 61.

128 H. Xu, B.H. Lee, K. Donovan, M. Wong, E.C. Franks, *China's New AI Regulations*, „Client Alert Commentary”, 3310/2023, <https://www.lw.com/en/admin/upload/SiteAttachments/Chinas-New-AI-Regulations.pdf>, dostęp: 8 stycznia 2024 r.

129 H. Xu, B.H. Lee, K. Donovan, M. Wong, E.C. Franks, *China's....*

130 H. Xu, B.H. Lee, K. Donovan, M. Wong, E.C. Franks, *China's....*

131 M. Sheehan, *China's AI Regulations and How They Get Made*, 2023, https://carnegieendowment.org/files/202307-Sheehan_Chinese%20AI%20gov.pdf, dostęp: 8 stycznia 2024 r.

132 Zob. w tłumaczeniu na język angielski <https://digichina.stanford.edu/work/translation-artificial-intelligence-law-model-law-v-1-0-expert-suggestion-draft-aug-2023/>, dostęp: 8 stycznia 2024 r.

Podsumowując rozważania poświęcone chińskim doświadczeniom, można stwierdzić, że stanowią one zdecydowanie niedostatecznie doceniany przykład. **Obszerność istniejących regulacji jest z pewnością imponująca, zaś podejście w ramach którego reguluje się kazuistycznie kwestie szczegółowe,** składające się finalnie w kompleksowy system regulacji. Doświadczenia chińskie należy jednak brać pod uwagę z pewną poprawką na odmienny system prawno-polityczny obowiązujący w tym państwie.

3.7. Przykłady faktycznego zastosowania sztucznej inteligencji w bankowości światowej

Zagadnienie sposobów użycia AI w sektorze bankowym podejmowane jest w licznych publikacjach naukowych, w tym o charakterze systematycznych przeglądów literatury¹³³. Poniżej przedstawiono jednak najbardziej popularne, jak się zdaje, na chwilę obecną aplikacje systemów sztucznej inteligencji powszechnie wykorzystywanych w bankowości światowej. Ich rozwój wydaje się zaś być rzeczą absolutnie niemożliwą do uniknięcia. Nie oznacza to jednak, że działanie tych systemów nie rodzi lub nie będzie rodzić w przyszłości wątpliwości z punktu widzenia prawnego.

Niezwykle popularną formą stosowanego (zresztą nie tylko w bankowości, lecz również innych branżach, których przedsiębiorcy świadczą usługi masowe na rzecz konsumentów) narzędzia sztucznej inteligencji są boty, a w szczególności chatboty, czyli boty tekstowe oraz również boty głosowe. Co ciekawe, niezależnie od botów przeznaczonych dla zewnętrznych klientów banków, zdarza się również, że w banku funkcjonuje inny, wewnętrzny bot, który wspomagać może pracowników w rozwiązywaniu różnego rodzaju problemów, wynikających z procesów organizacyjnych, dostępu do danych itp. Przykładem może tu być **SEB (szwedzki bank komercyjny), który poza chatbotem dla klientów dysponuje również chatbotem przeznaczonym dla swoich pra-**

cowników do komunikacji związanej ze sprawami szeroko rozumianego IT¹³⁴. Pamiętać przy tym należy, że aby systemy te spełniały swoją rolę muszą być one stale monitorowane i udoskonalane. System taki jest przydatny i nie będzie powodował więcej problemów niż korzyści dopiero wówczas, gdy nie tylko będzie on udzielał odpowiedzi oraz wyjaśnień, których potrzebują korzystające z niego osoby, ale również, a wręcz przede wszystkim wtedy, gdy poprawność udzielanych odpowiedzi jest maksymalnie wiarygodna, pewna i prawdziwa. Pozostając jeszcze w tematyce botów warto zwrócić uwagę na boty głosowe, w ramach których banki niekiedy nie tworzą swoich autorskich rozwiązań, a jedynie adaptują na swoje potrzeby znane i sprawdzone na rynku narzędzia sztucznej inteligencji¹³⁵. Przykładowo z Siri¹³⁶ korzysta brytyjski Barclays. Hiszpańska Bankia S.A.P postawiła z kolei na integrację z Asystentem Google¹³⁷.

Robodoradztwo (ang. robo-advisory), zdefiniowane zresztą przez KNF jako „forma zautomatyzowanego doradztwa finansowego stosowana m.in. w obszarze usług inwestycyjnych, pożyczek i ubezpieczeń (...) oparta na zaawansowanych algorytmach z wykorzystaniem sztucznej inteligencji i narzędzi do analizy dużych zbiorów danych (big data)”¹³⁸ wykorzystywane jest już w bankowości światowej. W takim przypadku system sztucznej inteligencji dokonuje analizy sytuacji klientów oraz różnych opcji inwestycyjnych oraz proponuje te, które w danym przypadku wydają się najlepsze. Wykorzystanie takiego systemu nie dzieje się kosztem zatrudnionych doradców, ale ułatwia im pracę. Ta bowiem w wielu przypadkach zaczyna ograniczać się **do omówienia z klientem zaproponowanego przez system rozwiązania, na co wskazuje przykład banku inwestycyjnego Morgan Stanley**¹³⁹.

Narzędzie sztucznej inteligencji wykorzystujące biometrię mogą być używane już na samym początku banku z klientem, czy wręcz potencjal-

133 W szczególności na ten temat zob.: O.H. Fares, I. Butt, i S.H.M. Lee, *Utilization of artificial intelligence in the banking sector: a systematic literature review*, „Journal of Financial Services Marketing”, 4(28)/2023, s. 835–852 i przywołana tam literatura. Na marginesie warto dodać, że problematyka wykorzystania AI w sektorze bankowym była przedmiotem analizy w raporcie Zastosowanie sztucznej inteligencji w bankowości – szanse oraz zagrożenia, sygn. WIB PAB 12/2022, https://us.edu.pl/wp-content/uploads/pliki/PAB_WIB_Zastosowanie_sztucznej_inteligencji_w_bankowosci_Szostek.pdf, dostęp: 7 stycznia 2024 r.

134 Raport *Sztuczna Inteligencja w Bankowości*, Warszawa 2020, <https://bank.pl/wp-content/uploads/2020/06/Raport-SZTUCZNA-INTELIGENCJA.pdf>, dostęp: 1 stycznia 2024 r., s. 24.

135 Raport *Sztuczna Inteligencja...*, s. 24–25.

136 Asystent głosowy Apple, dobrze znany części użytkowników tego ekosystemu.

137 Ten asystent głosowy znany jest z kolei użytkownikom mobilnego systemu operacyjnego Android.

138 <https://www.knf.gov.pl/dlarynku/fintech/roboradztwo>, dostęp: 9 stycznia 2024 r.

139 Raport *Sztuczna Inteligencja...*, s. 26.

nym klientem. Jeden z największych na świecie komercyjnych banków BBVA zastosował takie właśnie narzędzie, aby umożliwić swoim klientom założenie konta bez wyjścia z domu i wizyty w oddziale banku. Do realizacji tego celu potrzebny jest jedynie komputer z kamerą i odpowiednie prowadzenie klienta niejako „za rękę” przez narzędzie AI, które weryfikuje dokument tożsamości danej osoby oraz przeprowadza biometryczne porównanie twarzy z uwzględnieniem autentyczności osoby¹⁴⁰. W ramach takiego rozwiązania pamiętać jednak należy, aby zapewnić jego przystępność i łatwość obsługi z perspektywy klienta. Dopiero intuicyjna i satysfakcjonująca obsługa takiego systemu zapewni realizację celu, jakim jest pozyskanie klientów, za pomocą aplikacji bazujących na biometrii.

Poza obsługą klienta i ułatwianiem bieżącej pracy narzędzia AI wykorzystywane są również w kluczowym dla sektora finansowego aspekcie, tj. w aspekcie bezpieczeństwa. AI wspomaga wykrywanie oszustw w obszarze płatności, wyłudzeń środków finansowych oraz w ramach *phishingu*¹⁴¹. Również w zakresie **narzędzie AML (ang. anti-money laundering) narzędzia AI mogą znaleźć szerokie zastosowanie**¹⁴².

3.8. Wnioski z analizy komparatystycznej

Już ponad dwa lata temu wskazywano, że sztuczna inteligencja nie jest szeroko uregulowana prawnie, jednak oczekiwanie dalszych regulacji w tym zakresie uznać należy za zasadne¹⁴³. Uwaga ta w głównej mierze nie traci na swej aktualności pomimo odnotowanego w rzeczonym okresie postępu. Do zasadniczych wyzwań, dotyczących w równym stopniu wszystkich wyżej omówionych porządków prawnych, związanych ze stanowieniem prawa w obszarze nowych technologii z całą pewnością należy **kwestia skonstruowania definicji legalnej pojęcia „sztuczna inteligencja”**. Próby podania satysfakcjonującej definicji legalnej podjęte zostały w piśmien-

nictwie¹⁴⁴, a także prowadzone są inicjatywy mające na celu ujednolicenie siatki pojęciowej¹⁴⁵ w tym zakresie. Na tym jednak wyzwania dla podmiotów tworzących ramy prawne dla rozwoju i działania sztucznej inteligencji się nie kończą.

W tym miejscu należy również podkreślić istnienie, często przesłoniętych przez potencjalne korzyści, zagrożeń – nie tylko o charakterze czysto technicznym – związanych z wykorzystaniem AI w sektorze bankowym. Odnotowuje się przede wszystkim związek między digitalizacją i wdrażaniem SI w bankach a pogorszeniem warunków wykonywania pracy¹⁴⁶. Innowacyjność prowadzić może do zmian organizacyjnych w podmiotach sektora bankowego. Jak pokazuje przykład Francji, **wraz z reorganizacją modelu świadczenia usług bankowych (większy nacisk położono na usługi elektroniczne) część pracowników została zwolniona lub przeniesiona na inne stanowiska**¹⁴⁷. Natomiast postęp technologiczny nie sprawił, że pracownicy stali się zbędni. Zmniejszenie ich liczby doprowadziło jednak do zwiększenia obciążenia pracą osób, które zachowały swoje stanowiska.

Warto zaznaczyć, że **coraz szersze wykorzystanie rozwiązań opartych na SI wymaga posiadania przez pracowników określonych kompetencji, takich jak szybkość reakcji czy zdolność adaptacji, oraz umiejętności, jak np. automatyzacja pracy biurowej i (przynajmniej podstawowych) kompetencje z zakresu informatyki**¹⁴⁸. Natomiast dalszy rozwój SI wymaga specjalistycznej wiedzy z zakresu informatyki, przez co przypuszczalnie sektor bankowy dążyć będzie do nawiązania współpracy z wyspecjalizowanymi podmiotami zewnętrznymi. Opracowanie AI stanowi bowiem przedsięwzięcie długoterminowe, wymagające rygorystycznego oraz dobrze zapla-

144 Zob. J. Rzymowski, *Definicja prawnicza sztucznej inteligencji na podstawie projektu rozporządzenia w sprawie sztucznej inteligencji*, „Prawo Nowych Technologii”, 1/2023, s. 19 i n.; S. Szczepaniak, M. Brzostek-Kleszcz, *Definiowanie pojęć z zakresu nowych technologii w przepisach prawa i postanowieniach umownych*, „Prawo Nowych Technologii”, 2/2021, s. 66 i n.

145 W szczególności zob. <https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence>, dostęp: 13 grudnia 2023 r. Przedsięwzięcie to ma na celu uzgodnienie siatek pojęciowych z zakresu AI właściwych dla systemu prawnego USA oraz prawodawstwa unijnego.

146 Zob. C. Perez i F. Martin, *Digitalisation and Artificial Intelligence: the New Face of the Retail Banking Sector. Evidence from France and Spain*, 2018, s. 218-226.

147 *Ibid.*, s. 204.

148 Zob. S. Benhamou, *Artificial Intelligence and the Future of Work...*, *op. cit.*, s. 83.

140 Raport *Sztuczna Inteligencja...*, s. 57.

141 Raport *Sztuczna Inteligencja...*, s. 35.

142 Raport *Sztuczna Inteligencja...*, s. 63.

143 D. Ślażyńska-Kluczek, *Sztuczna inteligencja – regulacje prawne, miejsce w polskim sektorze bankowym*, „Nauki Ekonomiczne”, 34/2021, s. 54.

nowanego postępowania. Równie **korzystne wydaje się nawiązanie współpracy z uniwersytetami lub instytucjami badawczymi dysponującymi niezbędną w tym zakresie wiedzą, która pozwoli nie tylko na stworzenie odpowiednich dla sektora bankowego rozwiązań opartych na systemach sztucznej inteligencji, ale również przeszkolenie pracowników z właściwego ich użycia oraz przygotowanie instrukcji dla klientów**, których obsługę również prowadzi się z bezpośrednim wykorzystaniem i kontaktem z AI.

Przeprowadzona analiza doświadczeń poszczególnych państw w zakresie wykorzystania i uregulowania AI uwypukla **różnice w podejściu do stanowienia prawa sztucznej inteligencji w odmiennych kulturach i tradycjach prawnych**. Na przykładzie Francji i Niemiec wyraźnie widoczny jest związek prawodawstwa przede wszystkim z gwarancjami prawno-człowieczymi, w szczególności zaś ochroną prywatności. Trend ten, ze względu na oddziaływanie prawa unijnego będzie najprawdopodobniej charakterystyczny dla wszystkich państw członkowskich UE, a zatem również dla Polski. Postęp prac nad harmonizacją prawa unijnego w zakresie AI, szerzej omówiony w kolejnym rozdziale niniejszego raportu, pozwala przypuszczać, że w państwach członkowskich UE naczelną rolę odegra jeden, kompleksowy akt normatywny, nieco podobnie zresztą jak miało to miejsce w zakresie regulacji poświęconych problematyce ochrony danych osobowych. Z kolei rozwiązania prawne w USA kładą **większy nacisk na dookreślenie cech godnego zaufania systemu sztucznej inteligencji oraz zapewnieniu warunków dla dalszego rozwoju tej technologii, przy jednoczesnym konstruowaniu katalogu praw podstawowych związanych z SI**. W pewnym sensie regulacją o charakterze łączącym cechy właściwe prawodawstwu USA oraz państw członkowskich UE są niektóre rozwiązania projektowane w UK. Po pierwsze, warto dostrzec przyjęcie odmiennej strategii stanowienia prawa niż w UE. Proponuje się bowiem **wyznaczenie sektorowych ram regulacyjnych, zakotwiczonych w już istniejącej, rozproszonej sieci nie tylko regulatorów krajowych, ale także przepisów prawa stanowionego**.

Do najczęściej wykorzystywanych reakcji prawnych na naruszenia przepisów obowiązujących w związku z wykorzystaniem AI należą odpowiednio **dochodzenie praw na drodze postępowania sądowego (co widać przede wszystkim na przykładzie doświadczeń USA) oraz sankcje natury administracyjnoprawnej** (rozwiązanie to jest właściwe krajom,

w którym silna jest pozycja regulatorów sektorych lub wyspecjalizowanych agencji rządowych, a zatem mowa tutaj przede wszystkim o państwach Starego Kontynentu, w których prawo administracyjno-karne podlega stałemu rozwojowi¹⁴⁹).

Przykład Chin pokazuje inne podejście do zagadnienia regulacji AI. Tutaj nie tylko tworzenie prawa jest domeną państwa. Również rozwój AI skupiony jest w jego rękach. **Państwo stawia sobie za cel bycie przodownikiem w zakresie tak rozwijania jak i korzystania z systemów sztucznej inteligencji**. Z uwagi jednak na ograniczone zasoby państwo wykorzystuje również potencjał podmiotów prywatnych, zachęcając je do rozwijania się na rodzimym rynku i tworzenia pożądanych systemów w bardzo sprecyzowanych obszarach. Jednocześnie **regulacje poświęcone sztucznej inteligencji jako takiej zdają się być dużo bardziej szczegółowe (kazuistyczne, rozbudowane i relatywnie restrykcyjne) niż w pozostałych z omówionych systemów prawnych**. Docelowo zaś powstać ma jeden kompleksowy akt prawny, który ma za zadanie kompleksowo uregulować problematykę sztucznej inteligencji i działających w oparciu o nią systemów. W konsekwencji należy rekomendować stałe monitorowanie rozwiązań prawnych przyjętych przez Państwo Środka, gdyż mogą one okazać się niezwykle cenne i warte zaaplikowania również na gruncie rodzimym.

Przeprowadzając analizę komparatystyczną doświadczeń państw wywodzących się z różnych tradycji i hołdujących innym niekiedy wartościom nie można tracić z pola widzenia faktu, że kwestia optymalnej regulacji wykorzystania AI – nie tylko w sektorze bankowym, choć ten słusznie przedstawia się jako jeden z kluczowych obszarów szerszego stosowania sztucznej inteligencji – stanowi wyzwanie o charakterze globalnym. W tym świetle wydaje się, że zaakcentowane wyżej odmienności stanowią skutek różnego rozłożenia akcentów w debacie poświęconej dalszym kierunkom rozwoju SI. Do najistotniejszych wyzwań, powszechnie rozpoznawanych przez porównywane porządki prawne należą zagadnienia, takie jak: **zapobieganie dyskryminacji automatycznej, ochrona danych osobowych, czy ustalenie cech godnego zaufania systemu SI**. Trzeba także zaznaczyć, że regulacji niektórych kwestii, których prób unormowania można by się spodziewać, jeszcze powszechnie nie podjęto. Tutaj

149 Zob. D. Szumiło-Kulczycka, *Prawo administracyjno-karne*, Warszawa 2004, s. 18.

przykładu dostarcza **kwestia odpowiedzialności za funkcjonowanie AI**, która stała się jedynie przedmiotem eksperckiego projektu chińskiego aktu prawnego mającego docelowo kompleksowo regulować problematykę sztucznej inteligencji. Przed zaprezentowaniem praktycznych postulatów i rekomendacji płynących z niniejszej części raportu warto ww. zagadnienia zaprezentować w sposób syntetyczny.

Dyskryminacja automatyczna, czy też **dyskryminacja algorytmiczna**, stanowi wyzwanie związane z zapewnieniem reprezentatywności treści generowanych przez SI względem danych wejściowych przetwarzanych przez AI. Powyższe zagadnienie zostało w literaturze ujęte obrazowo poprzez wskazanie, że: „algorytmy oparte na uczeniu maszynowym są wykorzystywane do odnajdowania w ogromnych zasobach danych wzorów, które mogą być znaczące dla procesu podejmowania decyzji. Identyfikowane korelacje są wykorzystywane do czynienia pewnych przewidywań. Jednak korelacje te pokazują pewne zależności, które nie muszą być zarazem związkami przyczynowo-skutkowymi. Na przykład w danym miejscu pracy może istnieć generalna zależność między płcią a liczbą zrealizowanych projektów, zgodnie z którą na jedną kobietę przypadają dwa projekty rocznie, a na jednego mężczyznę – cztery. Nie będzie to jednak równoznaczne z wykazaniem przyczynowości »kobiety robią mniej projektów, ponieważ są mniej wydajne zawodowo«, lecz będzie za tym stała okoliczność, zgodnie z którą kobiety częściej niż mężczyźni pracują na część etatu, zatem spędzają w pracy stosunkowo mniej czasu niż mężczyźni. Jeśli jednak algorytm, na podstawie którego podejmowane są decyzje kadrowe, powiąże wydajność pracy z płcią, będzie to wzmacniało istniejące nierówności między płciami i prowadziło do dalszej dyskryminacji”¹⁵⁰. Opisany tutaj mechanizm wskazuje w istocie na dwa – uniwersalne w tym sensie, że mogące dotyczyć różnych systemów sztucznej inteligencji niezależnie od sposobów ich użycia – źródła dyskryminacyjnego działania AI. Po pierwsze, zagrożenie dyskryminacji wiązać się może z powielaniem utrwalonych w danych wejściowych uprzedzeń¹⁵¹. Z tego względu, opracowując modele sztucznej inteligencji twórcy AI powinni działać w oparciu o duże objętościo-

wo zbiory danych. Po drugie, zniekształcenia mogą być wprowadzane przez sam algorytm stosowany przez SI. W tym zakresie zaleca się **stały nadzór nad treściami generowanymi przez SI i zapewnienie możliwości następcej ingerencji w model SI**.

Ochrona danych osobowych w kontekście sztucznej inteligencji stanowi nieustanne wyzwanie, które wymaga uwzględnienia i dostosowania istniejących przepisów prawnych. Wspomniano już, że twórcy systemów sztucznej inteligencji korzystają z danych, jednak zasadniczym elementem jest zagwarantowanie, że proces pozyskiwania tych danych jest zgodny z normami etycznymi i prawem. Niezwykle istotne jest, aby **respektować prawa do prywatności i ochrony danych osobowych**, zwłaszcza w kontekście, gdzie dane osobowe lub własność intelektualna są wykorzystywane w procesie trenowania sztucznej inteligencji. Proces ten musi być **transparentny, a uczestnicy powinni być świadomi, w jaki sposób ich dane są gromadzone, przetwarzane i wykorzystywane**. W kontekście państw członkowskich UE szczególne znaczenie ma RODO. Akt ten ustanawia przepisy dotyczące zbierania, przetwarzania i przechowywania danych osobowych, a także nadaje jednostkom prawo do kontroli nad swoimi danymi. W związku z tym, w obszarze sztucznej inteligencji, twórcy i operatorzy systemów muszą zastosować się do wymogów RODO, dbając o odpowiednie procedury związane z ochroną prywatności.

Zapewnienie spójności między różnymi jurysdykcjami i dostosowanie przepisów do dynamicznego rozwoju technologii sztucznej inteligencji stanowi kluczowy element zabezpieczający interesy jednostek oraz zachowujący równowagę między postępem technologicznym a prawami jednostek. W miarę jak technologia rozwija się, istotne jest, aby prawo ewoluowało wraz z nią, zapewniając skuteczną ochronę danych osobowych.

Ustalenie cech godnego zaufania systemu sztucznej inteligencji jest w swej istocie zadaniem nauki. Prawodawca, jeżeli decyduje się na kodyfikację pewnych własności cech AI powinien czynić to mając na względzie wytyczne specjalistów. W tym kontekście cenne jest AI RMF, które zwięźle podsumowuje aktualny dorobek naukowy i wskazuje pożądane cechy AI określając je jako: **prawidłowość i niezawodność, zapewnianie bezpieczeństwa użytkownikom systemu, odporność systemu na zagrożenia zewnętrzne i zdolność do przywrócenia prawidłowego działania, rozliczalność i przejrzystość, interpretowalność, ochrona prywatności i sprawiedliwość**.

150 A. Cybulko, *Dyskryminacja algorytmiczna w Polsce i możliwości przeciwdziałania jej na podstawie obowiązujących regulacji prawnych*, [w:] *Równouprawnienie. Księga pamiątkowa dla Profesory Małgorzaty Fuszary*, A. Krajewska i M. Rawłuszko (red.), Warszawa 2022, s. 286.

151 Zob. J. Niklas, *Problem dyskryminacji automatycznej – uwagi na tle ogólnego rozporządzenia o ochronie danych osobowych*, „Europejski Przegląd Sądowy”, 7/2019, s. 5.

3.9. Rekomendacje dla projektodawców oraz prawodawców regulacji AI na podstawie analizy komparatystycznej

Warto także zwrócić uwagę na niektóre zagadnienia, które wbrew intuicji nie są na tym etapie rozwoju SI przez prawodawców krajowych szczegółowo rozważane. Mowa tutaj przede wszystkim o zasadach odpowiedzialności za szkody wyrządzone przez funkcjonowanie AI, co szczególnie istotne jest w odniesieniu do automatyzacji – choć może w odniesieniu do SI trafniejsze byłoby sformułowanie „autonomizacji” przy zawierania transakcji¹⁵². Kontrowersje może budzić przypisanie odpowiedzialności za samą transakcję podmiotowi wykorzystującemu AI, skoro, inaczej niż ma to miejsce w przypadku „tradycyjnego” oprogramowania, SI zdolne jest do podejmowania decyzji niezależnych od pierwotnie wyznaczonego przez podmiot wykorzystujący AI, ram funkcjonowania systemu sztucznej inteligencji. W szczególności **samoucząca się sztuczna inteligencja może być w stanie, a nawet powinna, stale redefiniować te ramy w celu zapewnienia efektywności modelu**, co może stanowić dodatkową komplikację przedmiotowej kwestii.

Zanim jednak przystąpi się do szczegółowej regulacji problematyki AI, w tym w sektorze bankowym, warto zastanowić się, jakie już obowiązujące przepisy mogą być stosowane do zmieniającego się technologicznie świata oraz jakie są konsekwencje ich zastosowania, tj. jakie normy prawne dotyczące tak tworzenia systemów sztucznej inteligencji, korzystania z nich, jak i innych łączących się z tym zagadnień, w istocie obowiązują. Pamiętać bowiem należy, że nowa regulacja nie będzie działała w próżni prawnej, ale będzie częścią już obowiązującego systemu, a co za tym idzie jej struktury normatywne mogą i zapewne będą współtworzone przez już istniejące i obowiązujące przepisy.

Niezależnie od tego koniecznym może okazać się wydanie przepisów, które regulować będą precyzyjnie już tylko kwestie systemów sztucznej inteligencji. Inspiracją w tym zakresie z pewnością mogą być USA. Idąc ich przykładem warto zastanowić się nad tym, czy nie byłoby warto normatywnie określić

standardy stawiane przed systemami sztucznej inteligencji oraz wprowadzić normy prawne zapewniające odpowiedzialny rozwój i mechanizmy wdrażania sztucznej inteligencji.

Dodatkowo idąc śladem Zjednoczonego Królestwa warto w szczególności w zakresie AI, który w istotny sposób dotyka poszczególne jednostki oraz ich funkcjonowanie w różnych sferach, w tym na rynku pracy, przeprowadzić szerokie konsultacje społeczne. Z uwagi na to, że sztuczna inteligencja jest obecnie powszechnie dostępna i wiele osób ma z nią pewne doświadczenia, w tym osoby z sektora bankowego w sferze zawodowej, wsłuchanie się w głos takich osób może być niezwykle cenne i pomocne. Wskazanie na istniejące, jak i potencjalne problemy tak prawne, jak i technologiczne, przyczyniłoby się do stworzenia regulacji odpowiadającej na istniejące problemy tak o charakterze podstawowym, jak i szczegółowym. Cenną intuicją wyrażoną w toku wspomnianych konsultacji jest ponadto **potrzeba stałego monitorowania oraz bieżącego „doregulowywania” zagadnień rodzących się wraz z rozwojem technologii jaką jest SI lub przynajmniej dostarczania wytycznych, pozwalających na rozsądną, dostosowaną do bieżących wyzwań technologicznych, wykładnię obowiązującego prawa**.

Rozwiązania bazujące na sztucznej inteligencji są już dziś powszechnie stosowane w bankowości światowej. Z jednej strony służą one automatyzacji obsługi klientów, z drugiej ułatwiają pracę analityczną pracownikom banków. Nie sposób obecnie jakkolwiek zatrzymać tej rewolucji technologicznej, ale z pewnością warto wprowadzić ją w określone ramy po to, aby zapewnić bezpieczeństwo danych osobowych oraz przestrzeganie standardów prawnocząlowiecznych.

Mającą istotne znaczenie jest również kwestia **jednolitego standardu obowiązku informacyjnego w szczególności w przypadku, gdy sztucznej inteligencja wykorzystywana jest do obsługi klientów banku**. W takim przypadku klient powinien wiedzieć, że obsługiwany jest w ten właśnie sposób oraz jakie są tego konsekwencje. Co więcej, pojawia się istotne pytanie, czy banki, jak również inne instytucje, powinny mieć dowolność decydowania o tym, czy w danym przypadku za obsługę będzie odpowiadał konkretny człowiek czy sztuczna inteligencja, czy też możliwość obsługi przez sztuczną inteligencję powinna być poprzedzona zgodą (choćaby milcząco) konkretnego klienta.

¹⁵² Co do kwestii związanej z możliwością takiego właśnie wykorzystania AI zob. J. Mmereole, *Zawarcie umowy przez inteligentne oprogramowanie - smart kontrakty*, „Prawo Nowych Technologii”, 1/2023, s. 30 i n.



Rozwój sztucznej inteligencji, to jednak nie tylko rozwiązania prawne, ale również, a wręcz przede wszystkim kwestie technologiczne. Aby możliwe było ich rozwijanie, jak również w celu zachęcenia do tego **warto zastanowić się nad programami grantowymi, w ramach której finansowana będzie działalność rozwojowa AI. Z jednej strony takie inicjatywy mogą być podejmowane przez państwo, z drugiej przez sam szeroko pojęty sektor bankowy.** W tym drugim zakresie działalność rozwojowa byłaby jednak ograniczona do potrzeb sektora. Innymi słowy tworzone w jej ramach byłyby narzędzia sztucznej inteligencji sprofilowane od razu pod działalność bankową.

Narzędzia sztucznej inteligencji, jak sama ich nazwa wskazuje, są jedynie narzędziami i ułatwiają życie, w tym wykonywanie pracy. Aby tak się jednak

stało muszą być one w sposób właściwy obsługiwane, stąd należy wyrazić zapatrywanie, że poza rozwojem samych narzędzi konieczny jest również rozwój kompetencji kadry, która będzie się nimi posługiwała. Z tego względu **banki powinny organizować dla swoich pracowników szkolenia tak ze sztucznej inteligencji w ogólności, aby osoby te wiedziały z czym mają do czynienia, jakie są szansa, a jakie zagrożenia wynikające z korzystania z tej technologii.** Nie można jednak również zapominać o szkoleniach z konkretnych narzędzi, którymi dany podmiot będzie się posługiwał. Stąd poza szkoleniami o charakterze ogólnym wskazane jest organizowanie przez pracodawców, jakimi są banki szkoleń dla pracowników z konkretnych narzędzi sztucznej inteligencji, które wykorzystują oni w swojej pracy zawodowej.

4. Stan prawny: obecny oraz kierunki zmian legislacyjnych





4.1. Uwagi wprowadzające

W związku z postępującym rozwojem AI jesteśmy świadkami nowej ery, ery sztucznej inteligencji. Dynamiczna ekspansja nowoczesnych technologii, która przenika każdą sferę życia stanowi determinantę tego jak kształtował się będzie krajobraz normatywny w Unii Europejskiej. Obecnie truizmem jest twierdzenie, że „wyścig” prawa z technologią jest nierówną walką. Procesy legislacyjne są niezwykle długotrwałe, a niczym niehamowany rozwój AI utrudnia stworzenie kompletnych i aktualnych regulacji prawnych.

W dzisiejszych czasach **stworzenie jednego globalnego „ekosystemu” prawnego regulującego AI jest niemożliwe**. Niemniej jednak dokonująca się transformacja technologiczna wymusiła na Unii Europejskiej podjęcie działań legislacyjnych, w celu ustanowienia zharmonizowanych przepisów dotyczących AI.

W kwietniu 2021 r. Komisja Europejska przedstawiła wniosek w sprawie Rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji¹⁵³ („AI ACT”). Po upływie dwóch lat od przedstawienia wniosku, Parlament Europejski w dniu 14 czerwca 2023 r. przyjął poprawki projektu AI ACT. Przyjęte przez europejskiego ustawodawcę poprawki, w teorii pozwalały nakreślić przyszłe ramy regulacyjne w zakresie AI. Rzeczywistość zweryfikowała te założenia 13 marca 2024 r., czyli w dniu, w którym Parlament Europejski przyjął ostateczny tekst AI ACT¹⁵⁴. Ostateczna wersja AI ACT zawiera szereg zmian w stosunku do poprzednich wersji. Wprowadzanie poprawek w ramach trwającego procesu legislacyjnego nie stanowi żadnego *novum*. Zaznaczyć jednak należy, że **AI ACT w wersji przyjętej przez Parlament znacząco różni się od jego pierwotnej wersji**.

Niepewność legislacyjna negatywnie przekłada się na sektor finansowy, który pomimo bieżącego „monitoringu” procesu prac nad AI ACT nie był w stanie

przygotować się na „nadchodzące tsunami legislacyjne”, które stawia szereg nowych wymogów.

Co warto podkreślić, AI ACT ma zostać ostatecznie zweryfikowany przez prawników, lingwistów oraz ekspertów od technologii i ma zostać przyjęte przed końcem kadencji (procedura sprostowania)¹⁵⁵. 17 kwietnia 2024 r. przyjęto *Sprostowanie do stanowiska Parlamentu Europejskiego przyjętego w pierwszym czytaniu w dniu 13 marca 2024 r. w celu przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/... ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniającego rozporządzenia (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)*.

Dodać należy, że AI ACT musi zostać formalnie przyjęty przez Radę. AI ACT ma wejść w życie 20 dni po publikacji w Dzienniku Urzędowym, a w pełni obowiązywać będzie 24 miesiące po jego wejściu w życie. Zaznaczyć jednak należy, że jest szereg wyjątków – obowiązki dotyczące systemów wysokiego ryzyka będą obowiązywać 36 miesięcy po wejściu w życie. Istnieje **uzasadnione wątpliwości, że przyjęta *vacatio legis* jest zbyt krótka**. Zwłaszcza, że AI ACT to obszerna, przełomowa regulacja, która w znaczący sposób wpłynie na sektor prywatny.

Przewidywać należy, że w najbliższym czasie **mogą powstać problemy interpretacyjne wynikające z niespójności językowej AI ACT**. Wystąpienie ewentualnych rozbieżności pomiędzy poszczególnymi wersjami językowymi znacząco utrudni dekodowanie poszczególnych norm prawnych. Tego rodzaju trudności interpretacyjne mogą pojawić się w związku z podjętą próbą uregulowania niezwykle skomplikowanej materii jaką jest AI.

Omawiane rozporządzenie ma stanowić odpowiedź na zagrożenia związane z AI oraz podnieść w sposób znaczący standardy jakości, wydajności i wiarygodności w związku ze stosowaniem AI.

Warto zauważyć, że uregulowanie kwestii AI nastąpiło w formie rozporządzenia. Zgodnie z art. 288

¹⁵³ Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206>, dostęp: 28 grudnia 2023 r.; tekst AI ACT po poprawkach: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html, dostęp: 28 grudnia 2023 r.

¹⁵⁴ Tekst AI ACT przyjęty przez Parlament Europejski, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.html, dostęp: 15 marca 2024 r.

¹⁵⁵ Komunikat prasowy Parlamentu Europejskiego z dnia 14 marca 2023 r., <https://www.europarl.europa.eu/news/pl/press-room/20240308IPR19015/akt-w-sprawie-sztucznej-inteligencji-poslowie-przyjmujace-przelomowe-przepisy>, dostęp: 15 marca 2024 r.



Traktatu Ustanawiającego Europejską Wspólnotę Gospodarczą¹⁵⁶: „Rozporządzenie ma zasięg ogólny. Wiąże w całości i jest bezpośrednio stosowane we wszystkich Państwach Członkowskich”.

Wybór takiego instrumentu prawnego przez unijne go ustawodawcę miał na celu **ujednoczenie praktyki stosowania nowych przepisów oraz doprecyzowanie definicji związanych z nowymi technologiami**.

Projekt AI ACT był w doktrynie określany jako: „kluczowy element unijnej polityki rozwijania i wykorzystywania w ramach całego jednolitego rynku bezpiecznej i legalnej sztucznej inteligencji zgodnej z prawami podstawowymi”¹⁵⁷.

Nie sposób negować tego, że AI ACT będzie mocno oddziaływać na sektor prywatny, w tym w szczególności na sektor bankowy. AI ACT nie tylko podejmuje kwestię zagrożeń związanych z AI, lecz również kreuje standardy ochrony osób fizycznych oraz określa stopień jakości, wiarygodności systemów wykorzystujących AI.

Choć nie jest możliwe przeanalizowanie wszystkich rozwiązań przewidzianych w AI ACT, zaprezentowane zostaną najistotniejsze.

[Definicja Systemu Sztucznej Inteligencji]

Stworzenie uniwersalnej i najlepszej z punktu widzenia technik legislacyjnych definicji AI jest niezwykle trudne. Postępujący rozwój nowoczesnych technologii, niuanse z dziedziny informatyki utrudniają znalezienie właściwego ujęcia definicyjnego AI.

Unia Europejska w ramach prowadzonych prac legislacyjnych nad AI ACT przeniosła ciężar dyskusji na zdefiniowanie systemów sztucznej inteligencji. Zastosowanie takiego zabiegu legislacyjnego kładzie akcent na praktyczne sposoby zastosowania sztucznej inteligencji. Zdaniem ustawodawcy unijnego zagwarantuje to pewność prawa, przy jednoczesnym zapewnieniu elastyczności umożliwiającej dostosowanie się do przyszłego rozwoju technologicznego.

W pierwotnej wersji projektu AI ACT w art. 3 pkt 1 oraz w Załączniku nr I wprowadzono następują-

cą definicje systemów sztucznej inteligencji, która oznaczała:

„oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję;

- a) mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego;
- b) metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) i systemy ekspertowe;
- c) podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji.”.

Co istotne, po 14 czerwca 2023 r. powyższa definicja uległa zmianie, a Załącznik nr I, który określał zakres technik oraz podejść został usunięty. W obecnej wersji Załącznik nr I stanowi wykaz unijnego prawodawstwa harmonizacyjnego.

Wersja AI ACT z czerwca 2023 r. definiowała AI w sposób zbliżony do definicji prezentowanej przez OECD. Po zmianach system sztucznej inteligencji: „oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii i który może – do wyraźnych lub dorozumianych celów – generować wyniki, takie jak przewidywania, zalecenia lub decyzje wpływające na środowiska fizyczne lub wirtualne”¹⁵⁸.

Zaznaczyć należy, że **poprzednia definicja systemów AI odwołująca się m.in. do technik i podejść wymienionych w Załączniku I zakładała, że wraz z postępującym rozwojem nowych technologii Załącznik I będzie na bieżąco aktualizowany, tak aby nowo powstałe systemy zostały zakwalifikowane jako systemy AI**. Bieżące aktualizowanie Załącznika I AI ACT byłoby zadaniem niezwykle trudnym

¹⁵⁶ Dz. U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.

¹⁵⁷ R. Bujalski, Akt o sztucznej inteligencji, Lex, 2023.

¹⁵⁸ https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html, dostęp: 15 marca 2024 r.



i z punktu widzenia zasad dobrej legislacji rozwiązaniem wadliwym. Legislacja jest procesem długotrwałym, perspektywnym (obliczonym na przyszłość), co w konsekwencji mogłoby się przełożyć na „dystansowanie się” nowoczesnych technologii w wyszczególnieniu z prawem.

Uprzednia definicja systemów AI zdaniem wielu ekspertów była zbyt szeroka, ponieważ obejmowała systemy, które nie powinny zostać objęte przedmiotowym zakresem definicji systemów sztucznej inteligencji.

W celu zapewnienia aktualności oraz uniwersalności unijny prawodawca zdecydował się na zmianę definicji.

Definicja systemu sztucznej inteligencji z czerwca 2023 r. wprowadziła wiele zmian w stosunku do pierwotnej wersji AI ACT. Po pierwsze, system sztucznej inteligencji jest systemem maszynowym. W pierwszej wersji AI ACT system AI definiowany był jako oprogramowanie, co w konsekwencji mogło doprowadzić do uznania, że nawet proste narzędzia wykorzystywane w sektorze prywatnym mogłyby być uznane za systemy sztucznej inteligencji. Po drugie, po czerwcowych poprawkach definicja zakładała, że system AI będzie zaprojektowany z różnym systemem autonomii. Autonomiczność systemów AI pozwala odróżnić AI od innych technologii, które nie przewidują zdolności do samodzielnego działania bez ingerencji człowieka. Po trzecie, system AI może generować wyniki, takie jak przewidywania, zalecenia lub decyzje wpływające na środowiska fizyczne lub wirtualne.

Z kolei zgodnie z przyjętą w marcu 2024 r. wersją AI ACT: „system AI” oznacza system maszynowy, zaprojektowany do działania z różnym poziomem autonomii, który może po wdrożeniu wykazywać **zdolność adaptacji i który – do wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne**¹⁵⁹.

Dodane do definicji pojęcie – „zdolność adaptacji” zostało wyjaśnione w innej części AI ACT wskazując, że: „Zdolność adaptacji, jaką system AI może wykazać po jego wdrożeniu, odnosi się do zdolności do samouczenia się, która umożliwia zmianę systemu w czasie jego użytkowania”.

Aktualna definicja wskazuje również, że system AI musi charakteryzować się cechą zdolności do wnioskowania, która odnosi się do procesu uzyskiwania wyników, takich jak predykcje, treści, zalecenia lub decyzje.

Zdaniem autorów niniejszego Raportu, **obecna definicja systemów sztucznej inteligencji w znacznej mierze mityguje ryzyko szybkiego zdezaktualizowania się omawianej regulacji w związku z postępującym rozwojem nowoczesnych technologii.** Uznać należy, że zmiana definicji w trakcie procesu legislacyjnego wynikała z próby powiązania unijnej definicji z dotychczasowymi pracami organizacji międzynarodowych zajmujących się AI. Określenie kluczowych cech AI odróżniających ją od „tradycyjnych” systemów oprogramowania to krok w dobrym kierunku. Niemniej jednak dopiero czas pokaże czy wprowadzona w AI ACT definicja jest dostosowana do rozwoju technologicznego.

[Systemy AI wysokiego ryzyka]

Omawiając proponowane zmiany legislacyjne należy w tym miejscu omówić podejście unijnego ustawodawcy do klasyfikacji systemów AI wysokiego ryzyka. Po czerwcowych poprawkach Parlamentu Europejskiego zmianie uległo podejście do sposobu ich kwalifikacji.

W aktualnej wersji do systemów wysokiego ryzyka zakwalifikowane zostaną systemy AI, które spełnią następujące warunki:

„a) system AI jest przeznaczony do stosowania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I lub system AI sam w sobie jest takim produktem;

b) produkt, w którym zgodnie z lit. a) związanym z bezpieczeństwem elementem jest system AI, lub system AI sam w sobie jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I – ocenie zgodności przez stronę trzecią w związku z wprowadzeniem tego produktu do obrotu lub oddania go do użytku”¹⁶⁰.

W art. 6 ust. 3 AI ACT przewidziano zasadę odstępowania zgodnie, z którą systemu AI nie uznaje się za sys-

159 Zob. art. 3 AI ACT https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.pdf, dostęp: 15 marca 2024 r.

160 Zob. art. 6 ust. 1 AI ACT, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.pdf, dostęp: 15 marca 2024 r.



tem wysokiego ryzyka, jeżeli nie stwarza on znaczącego ryzyka szkody dla zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych, w tym poprzez brak znaczącego wpływu na wynik procesu decyzyjnego. Przepis ten w dalszej części określa warunki (co najmniej jeden z nich musi być spełniony), aby nie zakwalifikować danego systemu AI do systemu wysokiego ryzyka. Zaznaczyć przy tym należy, że system AI o którym mowa w załączniku III zawsze uznaje się za system wysokiego ryzyka, w przypadku, w którym system ten dokonuje profilowania osób fizycznych.

Oprócz systemów wysokiego ryzyka określonych w art. 6 ust. 1 AI ACT za systemy wysokiego ryzyka uznaje się systemy AI, o których mowa w załączniku III.

Co szczególnie istotne dla sektora finansowego Załącznik III AI ACT wskazuje, na następujące systemy AI wysokiego ryzyka:

„1. Biometria, w zakresie, w jakim jej stosowanie jest dozwolone na podstawie odpowiednich przepisów unijnych lub krajowych:

a) systemy zdalnej identyfikacji biometrycznej.

Nie obejmuje to systemów AI przeznaczonych do stosowania przy weryfikacji biometrycznej, której jedynym celem jest potwierdzenie, że określona osoba fizyczna jest osobą, za którą się podaje;

b) systemy AI przeznaczone do stosowania przy kategoryzacji biometrycznej, według wrażliwych lub chronionych atrybutów lub cech lub na podstawie wywnioskowania tych atrybutów lub cech;

c) systemy AI przeznaczone do stosowania przy rozpoznawaniu emocji.

(...)

5. Dostęp do podstawowych usług prywatnych oraz podstawowych usług i świadczeń

publicznych, a także korzystanie z nich: (...)

b) systemy AI przeznaczone do stosowania do celów oceny zdolności kredytowej osób fizycznych lub ustalenia ich punktowej oceny kredytowej, z wyjątkiem systemów AI wykorzystywanych w celu wykrywania oszustw finansowych;”

Unijny ustawodawca po czerwcowych poprawkach, które „ostały” się w przyjętej przez Parlament wersji

uznał, że systemy AI stosowane w celu wykrywania oszustw nie będą kwalifikować się do systemów AI wysokiego ryzyka. W konsekwencji szereg obowiązków związanych z użyciem AI wysokiego ryzyka nie będzie miał zastosowania do AI wykrywającego nieprawidłowości finansowe.

Warto przy tym zaznaczyć, że zmiana nie uległa zasadzie, zgodnie z którą systemami AI wysokiego ryzyka będą systemy, które na podstawie innych przepisów prawa Unii Europejskiej, będą podlegać ocenie przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku.

Zgodnie z motywem 46 AI ACT systemy AI wysokiego ryzyka powinny być wprowadzane do obrotu w Unii, oddawane do użytku lub wykorzystywane **wyłącznie, gdy spełniają określone wymogi. Systemami AI, które mają znaczący szkodliwy wpływ na zdrowie, bezpieczeństwo i prawa podstawowe powinny być uznane za systemy AI wysokiego ryzyka.**

Wymogi te powinny zapewniać, aby systemy AI wysokiego ryzyka nie stwarzały niedopuszczalnego ryzyka dla istotnych interesów publicznych Unii uznanych w prawie Unii i przez nie chronionych, w tym: (i) praw podstawowych; (ii) demokracji; (iii) praworządności; (iv) środowiska. Podkreślenia wymaga, że prawa podstawowe chronione na mocy Karty Praw Podstawowych Unii Europejskiej to m.in.:

- ▶ godność człowieka;
- ▶ poszanowanie życia prywatnego i rodzinnego;
- ▶ **ochrona danych osobowych;**
- ▶ **niedyskryminacja;**
- ▶ prawa pracownicze;
- ▶ **ochrona konsumentów.**

Zgodnie z najnowszą wersją AI ACT (motyw 96) banki przed wprowadzeniem systemów AI wysokiego ryzyka zobligowane są do przeprowadzenia oceny skutków w zakresie praw podstawowych. Celem przeprowadzenia takiej oceny jest: (i) zidentyfikowanie konkretnych rodzajów ryzyka dla praw lub grup osób; (ii) określenie rodzaju środków, które mają należy podjąć w przypadku urzeczywistnienia się tego ryzyka.



Klasyfikacja systemów AI wysokiego ryzyka ma doniosłe znaczenie dla określenia obowiązków sektora finansowego, w tym w szczególności banków. Należy mieć na względzie, że zarządzanie ryzykiem w świetle projektu AI ACT powoduje, że **banki mogą występować jako dostawcy lub podmiot stosujący AI**.

W sektorze finansowym funkcjonują wewnętrzne zespoły R&D – *Research and Development*, które tworzą lub doskonalą produkty bankowe za pomocą nowoczesnych technologii. Projekt AI ACT definiuje dostawcę jako osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, **które opracowują system sztucznej inteligencji lub zlecają jego opracowanie w celu wprowadzenia go do obrotu lub oddania go do użytku pod własną nazwą handlową lub własnym znakiem towarowym – odpłatnie lub nieodpłatnie**.

Zasadnym jest zatem uznać, że w przypadku zespołów R&D **banki mogą zostać zakwalifikowane jako dostawca, co z kolei implikuje realizację obowiązków dostawcy, określonych w AI ACT**.

Zgodnie z AI ACT dostawca powinien ustanowić skuteczny system zarządzania jakością, zapewnić przeprowadzenie wymaganej procedury oceny zgodności, sporządzić odpowiednią dokumentację i ustanowić solidny system monitorowania po wprowadzeniu do obrotu. W świetle pozostałych wymagań dostawcy powinni być również zobowiązani do **posiadania systemu zgłaszania właściwym organom incydentów** lub wszelkich naruszeń prawa UE, **w tym chroniącego prawa podstawowe (m.in. prawa konsumenta)**, zaistniałych w związku ze stosowaniem ich systemów sztucznej inteligencji, oraz do podejmowania odpowiednich działań naprawczych.

Przyjęta wersja AI ACT nakłada obowiązek zapewnienia, aby odpowiedzialność za wprowadzenie do obrotu lub oddanie do użytku systemu sztucznej inteligencji wysokiego ryzyka brała na siebie konkretna osoba fizyczna lub prawna określona jako dostawca, **niezależnie od tego, czy ta osoba fizyczna lub prawna jest osobą, która zaprojektowała lub opracowała ten system**.

Oprócz powyższych obowiązków, kluczowe dla banków – w sytuacji, w której bank zostałby zakwalifikowany jako dostawca w myśl AI ACT, będą wymogi określone w art. 16 AI ACT.

Omawiany przepis zawiera niezwykle obszerny zakres obowiązków z bezpośrednim odesłaniem do innych artykułów AI ACT. W formułowanym kata-

logu obowiązków nałożonych na dostawców systemów AI wysokiego ryzyka wskazano m.in. na: (i) zapewnienie zgodności z wymogami określonymi w sekcji 2 tj. (wdrożenie systemu zarządzania ryzykiem, spełnienie kryteriów jakości danych wykorzystanych do trenowania AI; zapewnienie dokumentacji technicznej; prowadzenie rejestru zdarzeń; przejrzystość; nadzór ze strony człowieka; spełnienie kryteriów dokładności i cyberbezpieczeństwa); (ii) podawanie w systemie AI wysokiego ryzyka lub – przypadku gdy nie jest to możliwe – na jego opakowaniu lub w dokumentacji towarzyszącej, stosownie do przypadku, swoją nazwę, zarejestrowaną nazwę handlową lub zarejestrowany znak towarowy i adres, pod którym można się z nimi skontaktować; (iii) posiadanie systemu zarządzania jakością; (iv) prowadzenie dokumentacji technicznej; (v) przechowywanie rejestrów zdarzeń generowanych automatycznie przez ich systemy AI wysokiego ryzyka (jak określono w art. 19 AI ACT), gdy rejestry takie znajdują się pod ich kontrolą; (vi) zapewnienie, aby system sztucznej inteligencji wysokiego ryzyka poddano odpowiedniej procedurze oceny zgodności przed wprowadzeniem go do obrotu lub oddaniem go do użytku; (vii) sporządzenie deklaracji zgodności UE zgodnie z art. 47 AI ACT; (viii) wypełnienie obowiązków rejestracyjnych, o których mowa w art. 49 ust. 1 AI ACT; (ix) podjęcie niezbędnych działań naprawczych i wypełnienie obowiązku informacyjnego zgodnie z art. 20 AI ACT.

Zaznaczyć również należy, że zgodnie z Załącznikiem III AI ACT systemy AI wykorzystywane w obszarze zatrudnienia, zarządzania pracownikami tj.: (i) systemy AI przeznaczone do stosowania do celów rekrutacji lub wyboru osób fizycznych, w szczególności do celów umieszczania ukierunkowanych ogłoszeń o pracę, analizowania i filtrowania podań o pracę oraz do oceny kandydatów; (ii) systemy AI przeznaczone do stosowania do celów podejmowania decyzji wpływających na warunki stosunków pracy, decyzji o awansie i rozwiązaniu stosunku pracy, przydzielania zadań w oparciu o indywidualne zachowanie lub cechy osobowości lub charakter oraz do monitorowania lub oceny wydajności i zachowania osób pozostających w takich stosunkach **są systemami AI wysokiego ryzyka, ergo w przypadku ich stosowania przez sektor finansowy, podmioty będą zobowiązane do spełnienia określonych w AI ACT wymogów**.

W kontekście powyższej regulacji nie bez znaczenia dla sektora bankowego są inne przepisy AI ACT, które przewidują pewne udogodnienia dla sektora finansowego.

Co istotne, projektowany AI ACT reguluje proces związany z zarządzaniem ryzykiem, co implikować będzie dokonanie procesu identyfikacji ryzyk oraz zmapowanie dotychczasowych rozwiązań.

Obecnie w instytucjach bankowych funkcjonują systemy zarządzania ryzykiem – (banki podlegają Dyrektywie Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE¹⁶¹ (dalej jako: „**dyrektywa 2013/36 UE**”).

W celu zachowania spójności między AI ACT, a przepisami mającymi zastosowanie do instytucji kredytowych objętych dyrektywą 2013/36/UE, w motywie 158 AI ACT wskazano, że: „(...) *niektóre obowiązki proceduralne dostawców związane z zarządzaniem ryzykiem, monitorowaniem po wprowadzeniu do obrotu oraz dokumentowaniem należy również włączyć do istniejących obowiązków i procedur przewidzianych w dyrektywie 2013/36/UE. Aby uniknąć nakładania się przepisów, należy również przewidzieć ograniczone odstępstwa dotyczące systemu zarządzania jakością prowadzonego przez dostawców oraz obowiązku monitorowania nałożonego na podmioty stosujące systemy AI wysokiego ryzyka w zakresie, w jakim mają one zastosowanie do instytucji kredytowych objętych regulacją na mocy dyrektywy 2013/36/UE*”.

Obowiązki związane z zarządzaniem ryzykiem zostały określone w art. 9 AI ACT.

Na gruncie art. 9 AI ACT zauważyć należy, że system zarządzania ryzykiem będzie obejmował następujące etapy:

- ▶ **identyfikację i analizę znanego i dającego się racjonalnie przewidzieć ryzyka**, jakie dany system AI wysokiego ryzyka może stwarzać dla zdrowia, bezpieczeństwa lub praw podstawowych, kiedy system ten będzie stosowany zgodnie ze swoim przeznaczeniem;
- ▶ **oszacowanie i ocenę ryzyka**, jakie może wystąpić podczas wykorzystywania systemu AI wysokiego ryzyka zgodnie z jego przeznaczeniem

i w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania;

- ▶ **ocenę innego mogącego wystąpić ryzyka** na podstawie analizy danych zebranych z systemu monitorowania po wprowadzeniu do obrotu, o którym mowa w art. 72;
- ▶ **przyjęcie odpowiednich i ukierunkowanych środków zarządzania ryzykiem** zaprojektowanych w celu przeciwdziałania ryzyku zidentyfikowanemu zgodnie z art. 9 ust. 2 lit. a AI ACT.

Powyższe regulacje oznaczają, że **sektor bankowy będzie musiał powołać odpowiednie zespoły, które zidentyfikują ryzyka oraz dostosują wewnętrzne procedury do AI ACT**.

Projekt rozporządzenia określa również rodzaj najodpowiedniejszych środków do zarządzania ryzykiem, które mają zapewnić:

- ▶ eliminację lub ograniczenie zidentyfikowanego ryzyka, o ile jest to wykonalne pod względem technicznym, poprzez odpowiednie zaprojektowanie i opracowanie systemu sztucznej inteligencji wysokiego ryzyka, w stosownych przypadkach przy udziale ekspertów i zewnętrznych zainteresowanych stron;
- ▶ w stosownych przypadkach wdrożenie odpowiednich środków służących ograniczeniu i kontroli ryzyka, którego nie można wyeliminować;
- ▶ dostarczenie wymaganych informacji – art. 13 AI ACT oraz w stosownych przypadkach, przeszkolenie podmiotów stosujących AI.

Zaznaczyć należy, że art. 13 AI ACT kładzie szczególny nacisk na przejrzystość, która ma umożliwić dostawcom i podmiotom stosującym AI interpretację wyników działania systemu. Przy czym, stopień przejrzystości ma być odpowiedni do przeznaczenia systemu sztucznej inteligencji w celu osiągnięcia zgodności z odpowiednimi obowiązkami dostawcy i podmiotu stosującego AI, które określono w sekcji 3 AI ACT. Z kolei w art. 50 AI ACT określono obowiązki w zakresie przejrzystości dla dostawców i użytkowników stosujących niektóre systemy AI.

Co ciekawe wersji AI ACT z czerwca 2023 r. w art. 13 dookreślono, czym jest przejrzystość:

„Przejrzystość oznacza zatem, że w momencie wprowadzania do obrotu systemu sztucznej inteli-

¹⁶¹ Dz. U. UE. L. z 2013 r. Nr 176, str. 338 z późn. zm.



gencji wysokiego ryzyka wykorzystuje się wszystkie dostępne środki techniczne zgodnie z powszechnie uznanym aktualnym stanem wiedzy, aby zapewnić dostawcy i użytkownikowi możliwość interpretacji wyników systemu sztucznej inteligencji. Użytkownik musi być w stanie zrozumieć system sztucznej inteligencji oraz korzystać z niego na podstawie ogólnej wiedzy na temat sposobu funkcjonowania systemu sztucznej inteligencji i przetwarzanych przez niego danych, dzięki czemu będzie on mógł wyjaśnić decyzje podjęte przez system sztucznej inteligencji osobom, których decyzje te będą dotyczyć zgodnie z art. 68 lit. C).¹⁶²

W ostatnio przyjętej przez Parlament Europejski wersji AI ACT, zrezygnowano z doprecyzowania, czym jest przejrzystość w art. 13 – na rzecz dookreślenia tego pojęcia w motywie 27, zgodnie z którym: „(...) Przejrzystość oznacza, że systemy AI opracowuje się i wykorzystuje w sposób umożliwiający odpowiednią identyfikowalność i wytłumaczalność, jednocześnie informując ludzi o tym, że komunikują się z systemem AI lub podejmują z nim interakcję, a także należy informować podmioty stosujące AI o możliwościach i ograniczeniach tego systemu AI, a osoby, na które AI ma wpływ, o przysługujących im prawach”¹⁶³.

Dodać również należy, że art. 13 ust. 2 AI ACT przewiduje obowiązek dołączenia do systemów AI wysokiego ryzyka instrukcji obsługi.

Warto również zwrócić uwagę na art. 9 ust. 10 AI ACT, który zakłada, że w odniesieniu do dostawców systemów AI wysokiego ryzyka, którzy podlegają wymogom dotyczącym wewnętrznych procesów zarządzania ryzykiem na podstawie innego odpowiedniego prawa Unii (np. instytucje kredytowe podlegające przepisom dyrektywy 2013/36/UE), aspekty przewidziane w ust. 1–9 mogą być częścią procedur zarządzania ryzykiem ustanowionych zgodnie z tym prawem lub łączyć się z tymi procedurami.

Jednocześnie w art. 17 ust. 4 AI ACT przewidziano, że: „W odniesieniu do dostawców będących instytucjami finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych, obowiązek

wprowadzenia systemu zarządzania jakością, z wyjątkiem ust. 1 lit. g), h) oraz i) niniejszego artykułu, uznaje się za spełniony w przypadku zapewnienia zgodności z przepisami dotyczącymi zarządzania wewnętrznego, uzgodnień lub procedur zgodnie z odpowiednimi unijnymi przepisami dotyczącymi usług finansowych. W tym celu uwzględnia się wszelkie normy zharmonizowane, o których mowa w art. 40”¹⁶⁴.

W doktrynie podkreśla się, że przywołane powyżej rozwiązanie stanowi „ułatwienie” w zakresie wdrożenia odpowiednich rozwiązań w sytuacji, w której „instytucja kredytowa ustanowi odpowiednie i specyficzne rozwiązania adresujące przepisy AI Act, to nie będzie zobowiązana do ustanawiania odrębnych polityk czy procedur w tym zakresie”¹⁶⁵.

[Podejście oparte na ryzyku – risk-based approach]

W AI ACT wielokrotnie pojawia się słowo „proporcjonalność” jednakże brak jest jednoznacznego odwołania się do praktycznych wskazówek związanych ze sposobem stosowania zasady proporcjonalności.

Niemniej jednak w motywie 27 AI ACT wskazano, że: „Chociaż podstawą proporcjonalnego i skutecznego zestawu wiążących przepisów jest podejście oparte na analizie ryzyka, należy przypomnieć Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji z 2019 r. opracowane przez niezależną grupę ekspertów wysokiego szczebla ds. AI powołaną przez Komisję. W tych wytycznych grupa ekspertów wysokiego szczebla ds. AI opracowała siedem niewiążących zasad etycznych dotyczących AI, które mają pomóc zapewnić, aby AI była godna zaufania i zgodna z normami etycznymi. **Te siedem zasad to: przewodnia i nadzorczą rolę człowieka; techniczna solidność i bezpieczeństwo; ochrona prywatności i zarządzanie danymi; przejrzystość; różnorodność, niedyskryminacja i sprawiedliwość; dobrostan społeczny i środowiskowy oraz odpowiedzialność (...)**”¹⁶⁶.

Skonstatować należy, że zasada proporcjonalności jest pojęciem nieostrym, a tym samym może powodować wiele problemów interpretacyjnych w szcze-

162 https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html, dostęp: 15 marca 2024 r.

163 https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.pdf, dostęp: 15 marca 2024 r.

164 Zob. art. 17 ust. 4 AI ACT, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.pdf, dostęp: 15 marca 2024 r.

165 M. Nowakowski, *Proces oceny zdolności kredytowej a AI Act [w:] Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023.

166 Zob. motyw 27 AI ACT, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.pdf, dostęp: 15 marca 2024 r.

gólności, gdy projektowane rozporządzenie stanowi swoiste *novum*. Dlatego bardzo ważną rolę będą odgrywały argumenty, które usprawiedliwią użycie danego systemu i jego proporcjonalność w konkretnym stanie faktycznym. Dopóki nie powstaną wytyczne w sprawie wdrożenia AI ACT istnieje szereg niewiadomych dotyczących praktycznego wdrażania rozporządzenia.

Jak czytamy w dokumencie roboczym służb komisji - streszczeniu sprawozdania z oceny skutków: „**Wniosek jest proporcjonalny i niezbędny do osiągnięcia celów, ponieważ zastosowano w nim podejście oparte na analizie ryzyka, a obciążenia regulacyjne nakłada się tylko w przypadku, gdy systemy sztucznej inteligencji mogą stwarzać wysokie ryzyko dla praw podstawowych lub bezpieczeństwa. W przeciwnym razie nakłada się jedynie minimalne obowiązki w zakresie przejrzystości, w szczególności w zakresie dostarczania informacji w celu zasygnalizowania wykorzystania systemu sztucznej inteligencji przy kontaktowaniu się z ludźmi lub korzystania z technologii deepfake, jeśli nie stosuje się ich w uzasadnionych celach. Normy zharmonizowane oraz towarzyszące im wytyczne i narzędzia zapewniające przestrzeganie przepisów będą służyć wspieraniu dostawców i użytkowników w spełnieniu wymogów oraz zminimalizują ich koszty**”¹⁶⁷.

Zaznaczyć należy, że dopiero ostateczny kształt AI ACT (przyjęty przez Radę po ewentualnym uwzględnieniu poprawek prawników – lingwistów) oraz jego praktyczne zastosowanie umożliwi dokonanie jednoznacznej oceny w zakresie przyjęcia przez UE adekwatnego ciężaru nakładanych obowiązków. Niemniej jednak obecny kształt AI ACT uznać należy, za „obciążający” regulacyjnie jego adresatów.

AI ACT zawiera szereg obowiązków i wymogów regulacyjnych w szczególności w zakresie ryzyka. Podmioty rynku finansowego oraz podmioty, które świadczą na rzecz instytucji finansowych swoje usługi technologiczne (Fintech, RegTech) będą musiały spełnić nadchodzące wymogi regulacyjne.

W uzasadnieniu projektu AI ACT dot. analizy ryzyka wskazano, że: „ryzyko powinno być obliczane z uwzględnieniem wpływu na prawa i bezpieczeństwo”¹⁶⁸.

Zasadę podejścia opartego na analizie ryzyka oraz odwołanie do proporcjonalności można odnaleźć w motywie 26 preambuły AI ACT, wedle którego: „**Aby wprowadzić proporcjonalny i skuteczny zestaw wiążących przepisów dotyczących systemów AI, należy zastosować jasno określone podejście oparte na analizie ryzyka.** Takie podejście powinno polegać na dostosowywaniu rodzaju i treści takich przepisów do intensywności i zakresu ryzyka, jakie mogą powodować systemy AI. Konieczne jest zatem wprowadzenie zakazu stosowania niektórych niedopuszczalnych praktyk z zakresu AI, określenie wymogów w odniesieniu do systemów AI wysokiego ryzyka i obowiązków spoczywających na odpowiednich operatorach oraz określenie obowiązków w zakresie przejrzystości w odniesieniu do niektórych systemów AI.”¹⁶⁹.

Na tym gruncie zauważyć należy, że AI ACT wymienia m.in:

- ▶ systemy AI nieakceptowalne – zakazane (art. 5 AI ACT);
- ▶ systemy AI wysokiego ryzyka;
- ▶ systemy AI inne niż systemy AI wysokiego ryzyka.

Niektórzy eksperci wyróżniają również systemy AI przeznaczone do wchodzenia w interakcję z osobami fizycznymi, które muszą spełniać wymóg przejrzystości¹⁷⁰. **Warto zauważyć, że AI ACT w wersji z 2023 r. wprost regulował kwestie związane z modelami generatywnymi takich jak np. ChatGPT.**

AI ACT w brzmieniu z czerwca 2023 r. w art. 3 pkt 1c wskazywał, że: „*model generatywny*” oznacza model systemu sztucznej inteligencji, który jest trenowany na szerokiej skali danych, jest zaprojektowany z myślą o ogólnym charakterze wyników i może być dosto-

¹⁶⁷ Dokument roboczy służb komisji streszczenie sprawozdania z oceny skutków towarzyszący dokumentowi: wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w Sprawie Sztucznej Inteligencji) i zmieniającego niektóre akty ustawodawcze unii, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52021SC0085>, dostęp: 29 grudnia 2023 r.

¹⁶⁸ <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52021SC0084>, dostęp: 2 stycznia 2024 r.

¹⁶⁹ Zob. motyw 26 AI ACT, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.pdf, dostęp: 15 marca 2024 r.

¹⁷⁰ M. Nowakowski, *Podejście oparte na ryzyku – risk-based approach [w:] Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023.



sowane do szerokiego zakresu odrębnych zadań”¹⁷¹. W związku z „uregulowaniem” w AI ACT kwestii modeli generatywnych, unijny ustawodawca w art. 28b AI ACT (w wersji z czerwca 2023 r.) określił szereg wymogów dla dostawców takich systemów.

Ostatecznie zdecydowano się na uregulowanie modeli sztucznej inteligencji na podstawie związanego z nimi potencjalnego ryzyka. Wprowadzono przepisy dotyczące modeli AI ogólnego przeznaczenia wprowadzając bardziej restrykcyjne zasady w zależności od stopnia występującego ryzyka związanego z danym zastosowaniem. Duże generatywne modele AI są typowym przykładem modelu AI ogólnego przeznaczenia, biorąc pod uwagę, że umożliwiają one elastyczne generowanie treści¹⁷².

Jak już wspomniano uprzednio, w art. 9 AI ACT określono szereg wymogów dotyczących systemów AI wysokiego ryzyka, w tym konstytuuje się wymóg dokonywania regularnego przeglądu i aktualizacji procesu zarządzania ryzykiem (art. 9 ust. 2 AI ACT).

W konsekwencji uznać należy, że powyższe regulacje mogą:

- ▶ oznaczać zwiększenie kosztów dla organizacji w zakresie zarządzania ryzykiem;
- ▶ wymagać przypisania odpowiednich zasobów kadrowych do mapowania ryzyk w celu wypełnienia nowych obowiązków nałożonych przez AI ACT;
- ▶ doprowadzić do nakładania nieproporcjonalnych kar przez organy nadzoru państw członkowskich UE, w związku z niedostosowaniem się przez podmioty finansowe do skomplikowanej sieci obowiązków.

[Sztuczna Inteligencja a nadzór człowieka]

Jednym z największych wyzwań regulacyjnych naszych czasów jest stworzenie skutecznych regulacji wdrażających nadzór ze strony człowieka nad AI. Co ciekawe, wedle najnowszych badań empirycznych, ludzie nie są w stanie prawidłowo wykonywać

przypisanych im funkcji nadzorczych¹⁷³. Badania wykazały, że ludzie źle radzą sobie z oceną dokładności prognoz algorytmicznych (ludzie nadmiernie polegają na algorytmach – *automation bias* albo niedostatecznie polegają na algorytmach – *algorithm aversion*)¹⁷⁴.

Warto odnotować, że jednym z podstawowych dokumentów określających „wytyczne” dla użycia algorytmów było opracowanie niemieckiego Federalnego Urzędu Nadzoru Usług Finansowych (BaFin), które określało zasady nadzorcze związane z wykorzystaniem algorytmów sztucznej inteligencji w sektorze finansowym¹⁷⁵. We wspomnianym dokumencie określono m.in. zasadę „*Putting the human in the loop*”, wedle której „**pracownicy powinni być wystarczająco zaangażowani w interpretację i wykorzystanie wyników algorytmów przy podejmowaniu decyzji**”. Zaznaczyć należy, że AI ACT zdaje się uwzględniać powyższą zasadę, niejako dookreślając ją i uzupełniając w przepisach regulujących nadzorowanie przez człowieka systemów AI.

Jak wynika z przeprowadzonych badań, **obecność człowieka w pętli decyzyjnej ma kluczowe znaczenie dla poziomu zaufania społeczeństwa do AI**¹⁷⁶.

AI ACT stawia duży nacisk na kwestie nadzoru AI przez czynnik ludzki. AI ACT wymaga nadzoru człowieka w szczególności w zakresie systemów AI wysokiego ryzyka, które powinny być zaprojektowane w taki sposób, aby w **okresie ich wykorzystania** były one skutecznie nadzorowane. Warto zaznaczyć, że osoby fizyczne, które będą pełnić „funkcję nadzorczą” muszą być specjalistami w dziedzinie AI – standard wymaganych kompetencji określa art. 4 AI ACT. Co istotne, środki w zakresie nadzoru mają być współmierne do ryzyka, poziomu autonomii i kontekstu stosowania danego systemu AI.

171 Zob. art. 3 pkt 1C AI ACT: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html, dostęp: 2 stycznia 2023 r.

172 Zob. motyw 99 AI ACT: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.pdf, dostęp: 15 marca 2024 r.

173 B. Green, *The flaws of policies requiring human oversight of government algorithms*, „Computer Law & Security Review”, 45/2022.

174 B. Green, *The flaws of policies requiring human oversight of government algorithms*, „Computer Law & Security Review”, 45/2022, zob. S. Mo Jones-Jang, Y.J. Park., *How do people react to AI failure? Automation bias, algorithmic aversion, and perceived controllability*, „Journal of Computer-Mediated Communication”, 2023; J. Laux, *Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act*, „AI & Society”, 2023.

175 https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_Prinzipienpapier_BDAI_en.html, dostęp: 28 grudnia 2023 r.

176 A. Naomi, *The importance of the assurance that “humans are still in the decision loop” for public trust in artificial intelligence: Evidence from an online experiment*, „Computers in Human Behavior”, 114/2021.



Jednocześnie należy mieć na względzie, że art. 21 AI ACT nakłada na dostawców systemów AI wysokiego ryzyka daleko idące w skutkach obowiązki naprawcze i informacyjne: „Dostawcy systemów AI wysokiego ryzyka, którzy uznają lub mają powody, by uznać, że system AI wysokiego ryzyka, który wprowadzili do obrotu lub oddali do użytku, nie jest zgodny z niniejszym rozporządzeniem, **niezwłocznie podejmują niezbędne działania naprawcze w celu, stosownie do przypadku, zapewnienia zgodności tego systemu, wycofania go z rynku, wyłączenia go lub wycofania z użytku.**”¹⁷⁷.

Natomiast aktualny art. 26 AI ACT stanowi, że podmioty stosujące systemy AI wysokiego ryzyka mają zapewnić nadzór ze strony człowieka nad systemami wysokiego ryzyka.

W tym miejscu warto podkreślić, że proponowana regulacja podnosi poziom obecnych standardów unijnych określonych w art. 22 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)¹⁷⁸ („**RODO**”). Zdefiniowanie zakresu nadzoru ludzkiego jest nie tylko ważne dla określenia obowiązków pomiędzy dostawcami sztucznej inteligencji a operatorami AI, podmiotami stosującymi AI. Ogólnie rzecz biorąc, ludzie mogą wpływać na wyniki decyzyjne systemu AI podczas całego jego cyklu życia, tj. przed, w trakcie lub retrospektywnie po oddaniu systemu AI do użytku¹⁷⁹.

[Przejrzystość i udostępnianie informacji]

Kwestie przejrzystości oraz wyjaśnialności działań AI są kluczowe dla unijnego ustawodawcy, co znajduje odzwierciedlenie w samej treści AI ACT. W unijnych ocenach skutków regulacji dotyczących AI ACT trafnie zidentyfikowano, że brak przejrzystości AI: „ze względu na złożoność lub sposób realizacji algorytmu w kodzie lub sposób realizacji aplikacji) **utrudnia monitorowanie, identyfikowanie i udowad-**

nianie możliwych naruszeń prawa, w tym przepisów prawnych chroniących prawa podstawowe”¹⁸⁰.

Dostrzeżone przez UE problemy w zakresie przejrzystości AI są od kilku lat przedmiotem dyskusji w debacie publicznej oraz naukowej. Przejrzystość kodu, danych i procesu rozwoju sztucznej inteligencji są niezbędnymi elementami dla skutecznego nadzoru ze strony człowieka¹⁸¹. Trafnie wskazuje się, że wyjaśnialna, przejrzysta AI wykorzystująca algorytmy jest kluczowa dla funkcjonowania mechanizmów zarządzania AI¹⁸².

Użycie zaawansowanego technologicznie AI zwiększa prawdopodobieństwo wystąpienia efektu tzw. czarnej skrzynki (*black box*). Termin czarnej skrzynki oznacza niezrozumienie, niewyjaśnialność sposobu działania algorytmu¹⁸³. Efekt czarnej skrzynki może spowodować wystąpienie nowych zagrożeń dla bezpieczeństwa oraz praw podstawowych, a w konsekwencji może doprowadzić do niepewności prawa dla przedsiębiorstw – w kontekście AI ACT oraz potencjalnie wolniejszego wdrażania nowoczesnych technologii przez sektor prywatny. Problem jaki generuje czarna skrzynka doprowadził do powstania idei *Explainable Artificial Intelligence* – XAI, czyli wyjaśnialnej AI¹⁸⁴.

Przepisy AI ACT wymagają, aby systemy AI wysokiego ryzyka były zaprojektowane i opracowane, w taki sposób, **aby zapewniona została wystarczająca przejrzystość ich działania, która umożliwi zrozumienie funkcjonowania systemu.**

W przedmiocie przejrzystości oraz obowiązków informacyjnych dotyczących systemów AI przeznaczonych do interakcji z człowiekiem (np. *chatboty*,

¹⁷⁷ Zob. art. 20 AI ACT https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.pdf, dostęp: 15 marca 2024 r.

¹⁷⁸ Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.

¹⁷⁹ J. Laux, *Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act*. AI & Soc (2023).

¹⁸⁰ Commission Staff Working Document Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52021SC0084> (dostęp: 03.01.2024 r.)

¹⁸¹ B. Green, *The flaws of policies requiring human oversight of government algorithms*, „Computer Law & Security Review”, 45/2022.

¹⁸² J. Laux, *Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act*. AI & Soc (2023); B. Green, *The flaws of policies requiring human oversight of government algorithms*, Computer Law & Security Review, Volume 45, 2022;

¹⁸³ A. Krasuski, *Status prawny sztucznego agenta, Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2020, s. 153.

¹⁸⁴ G. Bar, *Przejrzystość, w tym wyjaśnialność, jako wymóg prawny dla systemów Sztucznej Inteligencji*, dodatek „Monitor Prawniczy”, 20/2020, Legalis.



voiceboty) omówić należy projektowany art. 50 AI ACT. Wspomniany przepis nakłada **obowiązek poinformowania osoby fizycznej w odpowiednim czasie, w jasny i zrozumiały sposób o tym, że prowadzi ona interakcję z systemem sztucznej inteligencji**, chyba że jest to oczywiste z punktu widzenia osoby fizycznej, która jest dostatecznie poinformowana, uważna i ostrożna, z uwzględnieniem okoliczności i kontekstu korzystania.

W powyższym kontekście eksperci celnie konkludują, że: „ustalenie i ewentualne ograniczenie zdolności chatbota lub voicebota będzie kluczowe dla ustalenia odpowiedzialności oraz wyznaczenia kierunku zmian organizacyjnych i technicznych, a także nadzoru i kontroli człowieka”¹⁸⁵.

[Biometria]

Impulsem do upowszechnienia w sektorze finansowym zastosowań wykorzystujących rozwiązania biometryczne była rosnąca ilość oszustw płatniczych oraz konieczność wdrożenia rozwiązań bezpieczniejszych niż wykorzystanie haseł czy numerów PIN¹⁸⁶.

Warto odnotować, że do systemów AI wysokiego ryzyka, należy również zaliczyć **systemy AI z obszaru biometrii, w zakresie w jakim jej stosowanie jest dozwolone na podstawie odpowiednich przepisów unijnych lub krajowych** z wyłączeniem systemów AI przeznaczonych do stosowania przy weryfikacji biometrycznej, której jedynym celem jest potwierdzenie, że określona osoba fizyczna jest osobą, za którą się podaje. Co istotne, zgodnie z motywem 54 AI ACT do systemów wysokiego ryzyka nie powinny zostać zakwalifikowane systemy biometryczne, które mają być wykorzystywane wyłącznie, by umożliwić stosowanie środków cyberbezpieczeństwa i ochrony danych osobowych.

AI ACT odwołuje się do danych biometrycznych zdefiniowanych w art. 4 pkt 14 RODO. Zgodnie z RODO „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub be-

hawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Z kolei w art. 3 pkt 41-42 AI ACT zdefiniowano systemy zdalnej identyfikacji biometrycznej.

Wypada zaakcentować, że wykorzystywane systemów AI, do: „łączenia danych (w tym zdjęcia) na dokumencie z obrazem człowieka (jego twarzą) (...) bez wątplenia można zakwalifikować jako systemy AI służące do identyfikacji biometrycznej”¹⁸⁷, co wiązać się będzie z obowiązkiem spełnienia wymogów określonych w AI ACT.

Zgodnie z motywem 17 AI ACT pojęcie systemu zdalnej identyfikacji biometrycznej należy zdefiniować funkcjonalnie jako system AI służący do identyfikacji osób fizycznych bez aktywnego udziału tych osób, co do zasady na odległość, poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych, niezależnie od konkretnej stosowanej technologii oraz konkretnych wykorzystywanych procesów lub rodzajów danych biometrycznych. Co istotne, do tej kategorii nie należą systemy AI przeznaczone do weryfikacji biometrycznej, która obejmuje uwierzytelnianie, prowadzonej jedynie w celu potwierdzenia, że dana osoba fizyczna jest osobą, za którą się podaje, oraz potwierdzenia tożsamości osoby fizycznej wyłącznie w celu uzyskania dostępu do usługi, uruchomienia urządzenia lub uzyskania bezpiecznego dostępu do pomieszczeń – ustawodawca dokonał tego wyłączenia, ponieważ uznał, że systemy te w niewielkim stopniu wpływają na prawa podstawowe.

Dodać należy, że w przywołanym powyżej motywie dokonano rozróżnienia między systemami zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” a systemami zdalnej identyfikacji biometrycznej „post factum”, biorąc pod uwagę ich różne cechy i sposoby stosowania, a także różne związane z nimi zagrożenia. W przypadku systemów działających „w czasie rzeczywistym” pobranie danych biometrycznych, porównanie i identyfikacja następują niemal natychmiast lub w każdym razie bez znacznego opóźnienia.

185 M. Nowakowski, *Zasada przejrzystości w przypadku systemów wchodzących w interakcję z człowiekiem* [w:] *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023.

186 K. Sawicka, *Wykorzystanie biometrii w procesie uwierzytelniania użytkowników elektronicznych usług płatniczych*, „Monitor Prawniczy”, 23/2018, Legalis.

187 M. Nowakowski, *Zdalny onboarding klienta a AI Act* [w:] *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023.

Za obejście przepisów AI ACT uznano celowe wprowadzanie opóźnień do systemów działających w czasie rzeczywistym. Systemy identyfikacji „w czasie rzeczywistym” obejmują wykorzystanie materiału rejestrowanego „na żywo” lub „w czasie zbliżonym do rzeczywistego”, takiego jak materiał wideo generowany przez kamerę lub inne urządzenie o podobnej funkcjonalności.

Z kolei w przypadku systemów identyfikacji *post factum* dane biometryczne zostały już pobrane, a porównanie i identyfikacja następują ze znacznym opóźnieniem. Dotyczy to materiałów, takich jak zdjęcia lub nagrania wideo generowane przez kamery telewizji przemysłowej lub urządzenia prywatne, których rejestracji dokonano, zanim użyto systemu w stosunku do danej osoby fizycznej.

[Wyznaczenie krajowych organów nadzorczych]

Unijny ustawodawca w **art. 70 AI ACT wymaga od każdego państwa członkowskiego wyznaczenia organu notyfikującego oraz organu nadzoru rynku**. Wyznaczone organy mają zostać zorganizowane w sposób gwarantujący obiektywizm i bezstronność podejmowanych przez niego działań i wykonywanych przez niego zadań¹⁸⁸.

Jak wynika z art. 70 AI ACT krajowy organ nadzorczy będzie pełnił funkcję organu nadzoru rynku. Do zadań krajowego organu nadzoru będzie należeć m.in.: (i) dbanie o stosowanie i wdrożenie AI ACT; (ii) udzielanie porad dotyczących wdrażania AI ACT uwzględniając przy tym wytyczne i porady Rady ds. AI i Komisji; (iii) przyjmując zgłoszenia dotyczące poważnych incydentów; (iv) w przypadku systemów AI wysokiego ryzyka wprowadzanych do obrotu, oddawanych do użytku lub wykorzystywanych przez instytucje finansowe podlegające unijnym przepisom dotyczącym usług finansowych – sprawowanie nadzoru finansowego, w zakresie, w jakim wprowadzanie do obrotu, oddawanie do użytku lub wykorzystywanie danego systemu AI jest bezpośrednio związane ze świadczeniem tych usług finansowych; (v) egzekwowanie przestrzegania obowiązków wynikających z AI ACT.

W powyższym kontekście dodać należy, że AI ACT ustanawia Europejską Radę ds. Sztucznej Inteligencji, której głównym zadaniem będzie doradztwo Komisji i państwom członkowskim oraz za-

pewnienie wsparcia w celu ułatwienia spójnego stosowania AI ACT.

Warto również wspomnieć o ustanowionym na mocy decyzji Komisji¹⁸⁹ Europejskim Urzędzie ds. Sztucznej Inteligencji. Nowy urząd ma m.in. współpracować i wspierać krajowe organy nadzoru, wspomóc wdrażanie przepisów dotyczących zakazanych praktyk w zakresie AI i systemów AI wysokiego ryzyka oraz ujednolicać stosowanie AI ACT we wszystkich państwach członkowskich UE.

[Sankcje]

W motywie 168 AI ACT podkreślono, że uchybienie wymogom określonym w AI ACT powinno być egzekwowane poprzez nakładanie kar i innych środków egzekwowania prawa, a państwa członkowskie powinny wprowadzić wszelkie niezbędne środki, aby zapewnić wdrożenie przepisów, w tym poprzez ustanowienie skutecznych, proporcjonalnych i odstraszających kar za ich naruszenie.

Ponadto wskazano, że Europejski Inspektor Ochrony Danych powinien mieć uprawnienia do nakładania grzywnien na instytucje, organy i jednostki organizacyjne Unii objęte zakresem stosowania AI ACT.

Wedle art. 99 ust. 3 AI ACT, nieprzestrzeganie zakazu praktyk – określonych w art. 5 AI ACT, podlega administracyjnej karze pieniężnej w wysokości **do 35 000 000 EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 7% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego**, przy czym zastosowanie ma kwota wyższa.

Z kolei niezgodność systemu AI z nałożonymi: (i) obowiązkami dostawców (art. 16 AI ACT); (ii) obowiązkami upoważnionych przedstawicieli (art. 22 AI ACT); (iii) obowiązkami importerów (art. 23 AI ACT); (iv) obowiązkami dystrybutorów (art. 24 AI ACT); (v) obowiązkami podmiotów stosujących AI (art. 26 AI ACT); (vi) wymogami i obowiązkami jednostek notyfikowanych (art. 31 AI ACT, art. 33 ust. 1 AI ACT, art. 33 ust. 3 AI ACT, art. 33 ust. 4 AI ACT lub art. 34 AI ACT); (vii) obowiązkami dostawców i użytkowników w zakresie przejrzystości (art. 50 AI ACT) **podlega administracyjnej karze pieniężnej w wysokości**

188 Zob. art. 70 AI ACT.

189 Decyzja Komisji z dnia 24 stycznia 2024 r. ustanawiająca Europejski Urząd ds. Sztucznej Inteligencji C(2024) 390.



do 15 000 000 EUR lub – jeżeli naruszenia dokonuje przedsiębiorstwo – w wysokości do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot jest wyższa.

Natomiast za przekazywanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym i właściwym organom krajowym (w odpowiedzi na ich wezwanie) podlega się administracyjnej karze pieniężnej w wysokości **do 7 500 000 EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 1% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego**, przy czym zastosowanie ma kwota wyższa.

Warto zauważyć, że AI ACT przewiduje również kary pieniężne dla **dostawców modeli AI ogólnego przeznaczenia**.

Przyjęta przez Parlament Europejski wersja AI ACT zakłada, że przy podejmowaniu decyzji, czy nałożyć administracyjną karę pieniężną, oraz przy ustalaniu jej wysokości powinno uwzględnić się:

- ▶ charakter, wagę i czas trwania naruszenia oraz jego konsekwencje, przy uwzględnieniu przeznaczenia systemu sztucznej inteligencji, a także, w stosownych przypadkach, liczby poszkodowanych osób oraz rozmiaru poniesionej przez nie szkody;
- ▶ czy inne organy nadzoru rynku w co najmniej jednym innym państwie członkowskim nałożyły już na tego samego operatora administracyjne kary pieniężne za to samo naruszenie;
- ▶ czy inne organy nałożyły już administracyjne kary pieniężne na tego samego operatora za naruszenia innych przepisów prawa Unii lub prawa krajowego, w przypadku, gdy takie naruszenia wynikają z tego samego działania lub zaniechania stanowiącego odnośne naruszenie niniejszego rozporządzenia;
- ▶ wielkość operatora dopuszczającego się naruszenia, jego roczny obrót i udział w rynku;
- ▶ wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak bezpośrednio lub pośrednio powiązane z danym naruszeniem osiągnięte korzyści finansowe lub uniknięte straty;

- ▶ stopień współpracy z właściwym organem krajowym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych niepożądanych skutków;
- ▶ stopień odpowiedzialności operatora, z uwzględnieniem wdrożonych przez niego środków technicznych i organizacyjnych;
- ▶ sposób, w jaki właściwe organy krajowe dowiedziały się o naruszeniu, w szczególności czy i w jakim zakresie operator zgłosił naruszenie;
- ▶ umyślny lub wynikający z zaniedbania charakter naruszenia;
- ▶ wszelkie działania podjęte przez operatora w celu złagodzenia szkody poniesionej przez poszkodowane osoby.

Warto zaznaczyć, że powyższy katalog okoliczności, które powinny być brane pod uwagę przy ustalaniu wysokości kary administracyjnej jest znacznie szerszy niż ten, który został uprzednio ujęty w pierwotnej wersji AI ACT. Zdaniem autorów niniejszego Raportu, dodanie dodatkowych okoliczności, które powinny być brane pod uwagę przy wymierzeniu kary należy uznać za zasadne.

[PSD 3 oraz PSR]

Szeroko rozumiana otwarta bankowość została ujęta w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE¹⁹⁰ (dalej jako: „**PSD 2**”). Dyrektywa PSD 2 zawiera zarówno przepisy dotyczące świadczenia usług płatniczych przez dostawców usług płatniczych, jak i przepisy dotyczące udzielania zezwoleń jednej konkretnej kategorii dostawców usług płatniczych, mianowicie instytucjom płatniczym, oraz nadzoru nad dostawcami usług płatniczych należącymi do tej kategorii.

PSD 2 wprowadziła koncepcję *open banking*, co przekładało się na udostępnienie infrastruktury bankowej związanej z przechowywaniem środków

190 Dz. U. UE. L. z 2015 r. Nr 337, str. 35 z późn. zm.



klientów dla świadczenia usług płatniczych¹⁹¹. Katalog usług płatniczych określony w dyrektywie PSD 1 został poszerzony przez Dyrektywę PSD 2 o:

- ▶ usługę inicjowania płatności (PIS);
- ▶ usługę dostępu do informacji o rachunku (AIS).

W czerwcu 2023 r. Komisja Europejska zaproponowała projekt nowej Dyrektywy PSD 3¹⁹² i rozporządzenia w sprawie usług płatniczych¹⁹³ (*Payment Services Regulation*, dalej jako: „PSR”). Co istotne, nowe projekty ww. aktów są ze sobą „powiązane”, a przewidziane w projektowanych aktach normatywnych regulacje mają na celu:

- ▶ zwalczenie i ograniczenie oszustw płatniczych;
- ▶ poprawę praw konsumentów;
- ▶ usprawnienie funkcjonowania otwartej bankowości;
- ▶ zwiększenie skuteczności egzekwowania przepisów i ich wdrażania w państwach członkowskich;
- ▶ poprawę (bezpośredniego lub pośredniego) dostępu do systemów płatności i rachunków bankowych dla dostawców usług płatniczych spoza sektora bankowego.

Projekt PSD 3 zakłada nowelizację dyrektywy SFD¹⁹⁴: „która w zakresie definicji instytucji mogących być uczestnikami systemów wyznaczonych, w tym organizowanych przez banki centralne systemów płatności RTGS, włącza instytucje płatnicze – z wyjątkiem

*instytucji płatniczych korzystających z wyłączeń określonych w art. 34, 36 i 38 dyrektywy PSD 3*¹⁹⁵.

PSD 3 oraz PSR zakłada również zmiany w zakresie usług wypłacania gotówki – podmioty prowadzące sklepy detaliczne są zwolnione z wymogu posiadania zezwolenia na prowadzenie działalności jako instytucja płatnicza, w przypadku, gdy oferują (dobrowolnie) usługi wypłaty gotówki bez zakupu w swoich lokalach, jeżeli kwota wypłaconej gotówki nie przekracza 50 EUR.

Warto odnotować, że projekt PSR zakłada zmiany dotyczące usług otwartej bankowości m.in. dotyczące zapewnienia specjalnych interfejsów dostępu. Dostawcy usług płatniczych prowadzący rachunek będą musieli zapewnić – z wyjątkiem sytuacji nadzwyczajnych, które uniemożliwiają im prowadzenie rachunku – udostępnienie z wyprzedzeniem wszelkich zmian w specyfikacji technicznej ich specjalnego interfejsu. Z kolei art. 36 PSR określa wymogi dotyczące specjalnych interfejsów dostępu do danych.

Warto zauważyć, że w projektowanym art. 39 PSR przewidziano odstępstwa od obowiązku posiadania specjalnego interfejsu dostępu do danych – na wniosek dostawcy usług płatniczych prowadzącego rachunek, właściwy organ może zwolnić wnioskującego dostawcę usług płatniczych prowadzącego rachunek z obowiązku posiadania specjalnego interfejsu.

PSR reguluje również kwestie, w jakich przypadkach instytucja kredytowa będzie mogła odmówić otwarcia rachunku płatniczego lub zamykać rachunek płatniczy instytucji płatniczej dla jej agentów lub dystrybutorów lub dla ubiegających się o zezwolenie na działalność¹⁹⁶.

W ramach zaproponowanego pakietu regulacyjnego oprócz PSD 3 oraz PSR zaliczyć należy, rozporządzenie w sprawie ustanowienia cyfrowego euro oraz rozporządzenie w sprawie zasad świadczenia usług płatniczych w obszarze cyfrowego euro przez dostawców z państwo non-euro oraz rozporządzenie ustanawiające ramy dla dostępu do danych finansowych. Zaproponowany przez UE pakiet regulacji

191 https://www.knf.gov.pl/komunikacja/blog?articleId=83447&p_id=18, dostęp: 4 stycznia 2024 r.

192 Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie usług płatniczych i usług związanych z pieniądzem elektronicznym w ramach rynku wewnętrznego, zmieniająca dyrektywę 98/26/WE i uchylająca dyrektywy (UE) 2015/2366 i 2009/110/WE, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52023PC0366>, dostęp: 4 stycznia 2024 r.

193 Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego i zmieniające rozporządzenie (UE) nr 1093/2010, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52023PC0367&qid=1704366317710>, dostęp: 4 stycznia 2024 r.

194 Dyrektywa Parlamentu Europejskiego i Rady 98/26/WE z dnia 19 maja 1998 r. w sprawie zamknięcia rozliczeń w systemach płatności i rozrachunku papierów wartościowych (Dz. Urz. UE. L 166 z 11.6.1998, s. 45–50, z późn. zm.).

195 Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2023 r., Cykliczny materiał dla Zarządu NBP z października 2023 r., str. 5, https://nbp.pl/wp-content/uploads/2023/11/Ocena-i-polrocze_2023_31-10-2023.pdf, dostęp: 4 stycznia 2024 r.

196 Zob. art. 32 PSR.



będzie miał znaczący wpływ na funkcjonowanie krajowego systemu płatniczego.

[Projektowane przepisy dotyczące odpowiedzialności cywilnej do AI]

Omawiając przepisy AI ACT nie sposób pominąć innych aktów unijnych, które będą określać ramy regulacyjne dla AI w sektorze finansowym. Jak wynika z badań przeprowadzonych w 2020 r. kwestia odpowiedzialności stanowi jedną z trzech najważniejszych barier na drodze do korzystania z AI przez europejskie przedsiębiorstwa.

Wyniki badań wskazują, że 43% przedsiębiorstw planujących wdrożenie AI za najistotniejszą zewnętrzną przeszkodę uznaje się kwestie odpowiedzialności za szkodę wywołaną przez AI¹⁹⁷.

Unijny ustawodawca w projekcie Dyrektywy Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozazumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję, dalej jako: „AILD”)¹⁹⁸ trafnie wskazują, że: *„Obowiązujące przepisy krajowe dotyczące odpowiedzialności, w szczególności opartej na zasadzie winy, nie są dopasowane do rozpatrywania roszczeń z tytułu odpowiedzialności za szkody spowodowane przez produkty i usługi oparte na sztucznej inteligencji. Zgodnie z tymi przepisami poszkodowani muszą udowodnić bezprawne działanie lub zaniechanie osoby, która spowodowała szkodę. Cechy szczególne sztucznej inteligencji, w tym jej złożoność, autonomia i brak przejrzystości (tzw. efekt czarnej skrzynki), mogą sprawić, że zidentyfikowanie osoby ponoszącej odpowiedzialność i udowodnienie spełnienia wymogów uznania roszczenia odszkodowawczego może być dla poszkodowanych trudne lub nadmiernie kosztowne. Poszkodowani ubiegający się o odszkodowanie mogą w szczególności ponieść bardzo wysokie koszty wstępne i uczestniczyć w znacznie dłuższym*

postępowaniu sądowym niż miałyby miejsce w sprawach niezwiązanych ze sztuczną inteligencją. Może to zatem powstrzymać poszkodowanych przed ubieganiem się o odszkodowanie”¹⁹⁹.

Projektowana Dyrektywa AILD zdaniem UE ma stanowić najodpowiedniejszy instrument, który zapewni pożądany skutek harmonizacji przepisów, pewność prawa oraz jednocześnie zapewni krajom członkowskim elastyczność umożliwiającą włączenie zharmonizowanych środków do krajowych systemów odpowiedzialności.

Dyrektywa AILD stanowi część tzw. pakietu środków mających sprzyjać wdrażaniu AI. W celu zachowania spójności z innymi regulacjami projektowana Dyrektywa AILD w art. 2 określającym szereg pojęć takich jak: systemy sztucznej inteligencji, system sztucznej inteligencji wysokiego ryzyka, dostawca, odwołuje się bezpośrednio do definicji zawartych w projekcie AI ACT – w brzmieniu AI ACT sprzed 14 czerwca 2023 r.

Co istotne w art. 3 AILD wprowadzono uprawnienie dla sądów krajowych do nakazania ujawnienia dowodów dotyczących systemów sztucznej inteligencji wysokiego ryzyka, co do którego istnieje podejrzenie, że spowodował szkodę, a powód spotkał się z odmową ujawnienia dowodów. Oznacza to większe prawdopodobieństwo potencjalnego przymusu ujawnienia dokumentacji związanej z systemami sztucznej inteligencji, tworzonej w kontekście AI ACT wobec instytucji nadzorczych. Oznacza to też dlatego konieczność dbałości o rzetelność takiej dokumentacji.

Warto podkreślić, że sądy krajowe mają ograniczać zakres ujawnianych informacji do tych dowodów, które są proporcjonalne i niezbędne, aby uzasadnić potencjalne lub wniesione roszczenie odszkodowawcze, oraz stosują jedynie takie zabezpieczenie dowodów, które jest proporcjonalne i niezbędne w celu uzasadnienia takiego roszczenia odszkodowawczego. Zaznaczyć należy, że od nakazu ujawnienia informacji będą przysługiwały środki ochrony prawnej pozwalające kwestionować nakaz. Dodać

197 European enterprise survey on the use of technologies based on AI [Badanie wśród europejskich przedsiębiorstw na temat stosowania technologii opartych na sztucznej inteligencji], Ipsos 2020, sprawozdanie końcowe, s. 58, <https://op.europa.eu/en/publication-detail/-/publication/f089bbae-f0b0-11ea-991b-01aa75ed71a1>, dostęp: 27 grudnia 2023 r.

198 Wniosek. Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozazumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), Komisja Europejska, 28.09.2022 r., COM (2022) 496 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022PC0496&from=EN>, dostęp: 27 grudnia 2023 r.

199 Wniosek. Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozazumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), Komisja Europejska, 28.09.2022 r., COM (2022) 496 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022PC0496&from=EN> (dostęp: 27.12.2023 r.).

należy, że zgodnie z projektowanymi przepisami niezastosowanie się do nakazu będzie skutkowało (wzruszalnym) domniemaniem braku zachowania należytej staranności.

Wskazać należy, że w art. 4 AILD wprowadzono wzruszalne domniemanie istnienia związku przyczynowego między winą pozwanego a wynikiem uzyskanym przez system sztucznej inteligencji lub faktem nieuzyskania przez taki system wyniku, jeżeli następujące warunki zostały kumulatywnie spełnione:

- i. udowodniono (albo przyjęto w drodze domniemania) winę pozwanego lub osoby, za którą on ponosi odpowiedzialność, polegającą na niedochowaniu obowiązku staranności określonego w prawie Unii lub w prawie krajowym i mającego bezpośrednio na celu ochronę przed zaistniałą szkodą;
- ii. w oparciu o okoliczności można uznać, że istnienie uzasadnione prawdopodobieństwo, iż wina wpłynęła na wynik uzyskany przez system AI lub na fakt nieuzyskania wyniku;
- iii. powód wykazał, że szkoda została spowodowana wynikiem uzyskanym przez system AI lub faktem nieuzyskania przez taki system wyniku²⁰⁰.

W kontekście powyższego warto dodać, że w przypadku roszczenia odszkodowawczego dotyczącego systemu sztucznej inteligencji wysokiego ryzyka sąd krajowy nie stosuje domniemania, jeżeli pozwany wykaze, że powód może uzyskać względnie łatwy dostęp do dowodów i wiedzy eksperckiej wystarczających, aby udowodnić związek przyczynowy.

Z kolei w przypadku roszczenia odszkodowawczego przeciwko dostawcy systemu sztucznej inteligencji wysokiego ryzyka podlegającemu wymogom określonym AI ACT (lub osobie podlegającej obowiązkowi dostawcy) **przesłanka winy jest udowodniona wyłącznie w przypadku, gdy którykolwiek z następujących wymogów nie został spełniony:**

- a) system sztucznej inteligencji wykorzystuje techniki obejmujące trenowanie modeli z wykorzystaniem danych, które nie zostały opracowane

na podstawie zbiorów danych treningowych, walidacyjnych i testowych spełniających kryteria jakościowe, o których mowa w art. 10 ust. 2–4 AI ACT (w brzmieniu sprzed 14 czerwca 2023 r.);

- b) system sztucznej inteligencji nie został zaprojektowany i opracowany w sposób spełniający wymogi w zakresie przejrzystości określone w art. 13 AI ACT (w brzmieniu sprzed 14 czerwca 2023 r.);
- c) system sztucznej inteligencji nie został zaprojektowany i opracowany w sposób umożliwiający osobom fizycznym jego skuteczne nadzorowanie w okresie wykorzystywania systemu sztucznej inteligencji zgodnie z art. 14 AI ACT (w brzmieniu sprzed 14 czerwca 2023 r.);
- d) system sztucznej inteligencji nie został zaprojektowany i opracowany w sposób umożliwiający osiągnięcie, z uwagi na jego przeznaczenie, odpowiedniego poziomu dokładności, solidności i cyberbezpieczeństwa zgodnie z art. 15 i art. 16 lit. a) AI ACT (w brzmieniu sprzed 14 czerwca 2023 r.) lub
- e) niezwłocznie nie podjęto niezbędnych działań naprawczych w celu zapewnienia zgodności systemu sztucznej inteligencji z obowiązkami określonymi w [tytule III rozdział 2 aktu w sprawie AI] lub, odpowiednio, w celu wycofania go z rynku lub wycofania go od użytkowników zgodnie z art. 16 lit. g) i art. 21 AI ACT (w brzmieniu sprzed 14 czerwca 2023 r.).

Jeżeli roszczenie będzie skierowane przeciwko użytkownikowi systemu AI wysokiego ryzyka przesłanka udowodnienia winy jest spełniona wówczas, gdy wykazano, że użytkownik:

- a) nie wywiązał się z obowiązku użytkowania lub monitorowania systemu sztucznej inteligencji zgodnie z załączoną instrukcją użytkowania lub, w stosownych przypadkach, z obowiązku wstrzymania lub przerwania jego użytkowania zgodnie z art. 29 AI ACT (w brzmieniu sprzed 14 czerwca 2023 r.) lub
- b) wprowadził do systemu sztucznej inteligencji dane wejściowe, nad którymi sprawuje kontrolę i które nie są adekwatne w odniesieniu do przeznaczenia tego systemu w rozumieniu art. 29 ust. 3 AI ACT (w brzmieniu sprzed 14 czerwca 2023 r.).

200 Zob. art. 4 AILD, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52022PC0496#footnote2>, dostęp: 27 grudnia 2023 r.



W przypadku roszczenia odszkodowawczego dotyczącego systemu sztucznej inteligencji, który nie jest systemem wysokiego ryzyka, domniemanie związku przyczynowego ma zastosowanie wyłącznie wtedy, gdy sąd krajowy uzna, że udowodnienie przez powoda związku przyczynowego jest nadmierne trudne. Ponadto wedle projektowanego AILD, gdy pozwanym jest osoba, która korzystała z systemu AI w ramach osobistej działalności pozazawodowej, domniemanie związku przyczynowego ma zastosowanie wyłącznie wówczas, gdy wpływała w istotny sposób na warunki działania systemu AI lub gdy miała taki obowiązek i tego nie uczyniła.

Eksperti wskazują, że projekt AILD: „jest mało przejrzysty, a jego rzeczywiste znaczenie w znacznym stopniu zależy od przyszłych losów i ostatecznego kształtu projektu Aktu w sprawie sztucznej inteligencji. Można jednak pokusić się o jego wstępną i generalną ocenę, która wypada raczej mało entuzjastycznie. Odnosi się on w zdecydowanie przeważającej części do systemów sztucznej inteligencji wysokiego ryzyka, czyli tych, z których działaniem wiąże się zagrożenie dla najistotniejszych dóbr człowieka albo istotne zagrożenie dla dóbr mniejszej wagi. Biorąc to pod uwagę, można zadać zasadnicze pytanie, czy porzucenie na odpowiedzialności opartej na winie jest trafną decyzją legislacyjną, nawet gdyby dochodzenie tej odpowiedzialności było ułatwione. Jak wynika z projektu, decyzja w kwestii zasady odpowiedzialności została odłożona na przyszłość co w praktyce oznacza, że obecnie pozostawiono ją prawodawcy krajowemu”²⁰¹.

W przypadku wejścia dyrektywy w życie państwa członkowskie będą zobowiązane do przyjęcia niezbędnych krajowych środków dostosowujących obecne systemy prawne do przepisów unijnych w ciągu dwóch lat. Ostateczny kształt AILD będzie uzależniony od przyjętej przez Parlament Europejski wersji AI ACT oraz dalszych prac legislacyjnych.

[Obecny stan prawny]

Obecnie jedną z największych zmian legislacyjnych na szczeblu unijnym jest nowo przyjęta Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/2225 z dnia 18 października 2023 r. w sprawie umów o kredyt konsumencki oraz uchylająca dyrekty-

wę 2008/48/WE²⁰² (dalej jako: „**CCD2**”). Państwa członkowskie UE mają dwa lata na implementację dyrektywy. CCD2, która zastąpi obecną dyrektywę w sprawie kredytu konsumenckiego – obowiązującą od 2008 r. Dyrektywa CCD2 bez wątpienia będzie miała wpływ na procesy związane z zarządzaniem danymi wykorzystywanych w szczególności do oceny zdolności kredytowej z użyciem rozwiązań opartych na AI.

W preambule CCD2 (motyw 46) wskazano: „*Jak podkreślono we wniosku Komisji dotyczącym rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji), opublikowanym w dniu 21 kwietnia 2021 r., systemy sztucznej inteligencji (AI) mogą być łatwo wprowadzane w wielu sektorach gospodarki i obszarach życia społecznego, w tym w wymiarze transgranicznym, i mogą znajdować się w obiegu w całej Unii. W tym kontekście kredytodawcy i pośrednicy kredytowi, personalizując cenę swoich ofert dla konkretnych konsumentów lub konkretnych kategorii konsumentów w oparciu o zautomatyzowane podejmowanie decyzji, powinni jasno informować konsumentów o tym, że proponowana im cena jest spersonalizowana na podstawie zautomatyzowanego przetwarzania danych osobowych, w tym danych wywnioskowanych, tak aby konsumenci mogli uwzględnić potencjalne ryzyka przy podejmowaniu decyzji o zakupie. Zgodnie z art. 14 ust. 2 lit. f) rozporządzenia (UE) 2016/679 kredytodawcy i pośrednicy kredytowi są również zobowiązani do informowania konsumentów, którzy otrzymują ofertę, o źródłach danych wykorzystywanych do personalizacji oferty*”²⁰³.

Zauważyć również należy, że CCD2 w motywie 56 bezpośrednio odwołuje się do systemów wysokiego ryzyka, o których mowa w AI ACT: „We wniosku Komisji w sprawie rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) określono, że systemy AI wykorzystywane do przeprowadzania punktowej oceny kredytowej lub oceny zdolności kredytowej osób fizycznych należy klasyfikować jako systemy AI wysokiego ryzyka, ponieważ decydują one o dostępie tych osób do zasobów finansowych lub podstawowych

202 Dz. U. UE. L. z 2023 r. poz. 2225

203 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/2225 z dnia 18 października 2023 r. w sprawie umów o kredyt konsumencki oraz uchylająca dyrektywę 2008/48/WE, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32023L2225>, dostęp: 27 grudnia 2023 r.

201 Na ten temat zob. P. Machnikowski, *Projekt dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję* [w:] *Prawo deliktowe wobec nowych technologii*, P. Machnikowski (red.), Warszawa 2023.

usług, takich jak mieszkalnictwo, energia elektryczna i usługi telekomunikacyjne. **W związku z tą wysoką stawką każdorazowo, gdy ocena zdolności kredytowej wiąże się ze zautomatyzowanym przetwarzaniem danych, konsument powinien mieć prawo do uzyskania interwencji ludzkiej ze strony kredytodawcy. Bez uszczerbku dla rozporządzenia (UE) 2016/679 konsument powinien mieć prawo do otrzymania rzeczowego, zrozumiałego wyjaśnienia dokonanej oceny oraz funkcjonowania zastosowanego zautomatyzowanego przetwarzania danych, w tym między innymi odnośnych głównych zmiennych, logiki i ryzyk, a także powinien mieć prawo do wyrażenia własnego stanowiska lub wystąpienia z wnioskiem o ponowną ocenę zdolności kredytowej oraz o ponowne rozpatrzenie decyzji w sprawie udzielenia kredytu. Konsument powinien mieć prawo do uzyskania informacji o tych prawach po należyтым otrzymaniu informacji na temat procedury, którą należy zastosować. Możliwość wystąpienia z wnioskiem o ponowne rozpatrzenie pierwotnej oceny i decyzji niekoniecznie powinna prowadzić do udzielenia konsumentowi kredytu**²⁰⁴.

W art. 18 ust. 8 CCD2 określono prawa jakie przysługują podmiotowi w przypadku wykorzystania zautomatyzowanego przetwarzania danych. Zgodnie z ww. art.: „**W przypadku, gdy ocena zdolności kredytowej obejmuje wykorzystanie zautomatyzowanego przetwarzania danych osobowych, państwa członkowskie zapewniają, aby konsument miał prawo zażądania i uzyskania od kredytodawcy interwencji człowieka, obejmujące prawo do:**

- a) **zażądania i uzyskania od kredytodawcy jasnego i zrozumiałego wyjaśnienia oceny zdolności kredytowej, w tym logiki i ryzyk uwzględnionych w toku zautomatyzowanego przetwarzania danych osobowych, a także jego znaczenia i wpływu na decyzję;**
- b) **przedstawienia kredytodawcy swojego stanowiska; oraz**
- c) **zażądania przeglądu oceny zdolności kredytowej i decyzji o udzieleniu kredytu przez kredytodawcę**²⁰⁵.

Powyżej przywołany artykuł jest zbliżony do wymogów zawartych RODO, określających jakie prawa przysługują podmiotowi w przypadku zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania.

Analizując w powyższym kontekście zasady zautomatyzowanego przetwarzania danych osobowych warto zwrócić uwagę na art. 105a ust. 1a ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe²⁰⁶ (dalej jako: „PB”), który stanowi: „Banki, inne instytucje ustawowo upoważnione do udzielania kredytów, instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, a także instytucje utworzone na podstawie art. 105 ust. 4, mogą w celu oceny zdolności kredytowej i analizy ryzyka kredytowego podejmować decyzje, opierając się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, danych osobowych - również stanowiących tajemnicę bankową - pod warunkiem zapewnienia osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz do wyrażenia własnego stanowiska”.

Porównując obecne zasady dotyczące zautomatyzowanego przetwarzania danych osobowych określonych w PB zasadnym jest stwierdzić, że CCD2 doprecyzowuje obowiązek wskazania czynników, które stanowiły podstawę wydanej decyzji. Kredytodawca będzie musiał przekazać konsumentowi jasne i zrozumiałe wyjaśnienie oceny zdolności kredytowej, **w tym logiki i ryzyk zawartych w toku zautomatyzowanego przetwarzania danych.**

Dyrektywa CCD2 reguluje również kwestie baz danych. W art. 19 ust. 1 CCD2 wskazano, że **w przypadku udzielania kredytu transgranicznego każde państwo członkowskie zapewnia kredytodawcom z innych państw członkowskich dostęp do baz danych wykorzystywanych w tym państwie członkowskim do oceny zdolności kredytowej konsumentów. Warunki dostępu do takich baz danych są niedyskryminujące**²⁰⁷. Podkreślić należy, że powyżej przywołany artykuł znajdzie zastosowanie do publicznych oraz prywatnych baz danych.

204 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/2225 z dnia 18 października 2023 r. w sprawie umów o kredyt konsumencki oraz uchylająca dyrektywę 2008/48/WE, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32023L2225>, dostęp: 27 grudnia 2023 r.

205 Zob. art. 18 ust. 8 CCD2, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32023L2225>, dostęp: 27 grudnia 2023 r.

206 Dz.U. z 2023 r. poz. 2488

207 Zob. art. 19 CCD2 <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32023L2225>, dostęp: 27 grudnia 2023 r.



Ponadto Dyrektywa CCD2 nakłada: (i) obowiązek zapewnienia przez państwa członkowskie, aby dostęp do baz danych mieli tylko ci kredytodawcy, którzy podlegają nadzorowi właściwego organu krajowego i w pełni przestrzegają RODO, (ii) obowiązek zapewnienia procedur skargowych przez państwa członkowskie do celów umów o kredyt dostawcy baz danych o kredytach, by ułatwić konsumentom składanie skarg na zawartość baz danych, w tym skarg dotyczących informacji, które osoby trzecie mogą uzyskać w drodze wyszukiwania w tych bazach danych.

Dodać również należy, że CCD2 rozszerza obowiązki dotyczące marketingu dla kredytów konsumenckich (reklama i marketing umów o kredyt).

[Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r., „CRD IV”]

Obecnie instytucje kredytowe podlegają przepisom dyrektywy CRD IV, które określają m.in. procedury związane z zarządzaniem ryzykiem. Warto zaznaczyć, że art. 9 ust. 9, art. 11 ust. 3a, art. 29 ust. 3 oraz ust. 5 AI ACT bezpośrednio odwołują się do Dyrektywy CRD IV. Uznać zatem należy, że dotychczasowa dokumentacja banków, która powstała na gruncie CRD IV stanowić będzie jeden z elementów dokumentacji wymaganej przez projektowane przepisy AI ACT.

[Akt w sprawie danych]

W dniu 22 grudnia 2023 r. opublikowano Rozporządzenie 2023/2854 w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828208 (akt w sprawie danych). Rozporządzenie weszło w życie 11 stycznia 2024 r. Ograniczone ramy niniejszego raportu nie pozwalają na omówienie wszystkich aspektów związanych z aktem w sprawie danych, niemniej jednak warto zaznaczyć, **że może on mieć wpływ w zakresie wprowadzonych zasad udostępniania danych.**

[Rozporządzenie DORA oraz Dyrektywa NIS2]

Omawiając kwestie związane z wykorzystaniem nowoczesnych technologii w sektorze finansowym, nie sposób pominąć w rozważaniach Rozpo-

ządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011209 (dalej jako: „DORA”) oraz Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148210 (dalej jako: „Dyrektywa NIS 2”) (Dz.U. UE. L. z 2022 r. Nr 333, str. 80).

Dora ustanawia wymogi dot. bezpieczeństwa sieci, usług związanych z ICT (technologiami informacyjno-komunikacyjnymi) oraz kwestie dot. zgłaszania poważnych incydentów związanych z ICT. Określone w DORA wymogi dot. zarządzania ryzykiem będą przekładać się na obecnie funkcjonujące systemy w instytucjach finansowych.

Zakres stosowania DORY obejmuje m.in. następujące podmioty finansowe:

- ▶ instytucje kredytowe;
- ▶ instytucje płatnicze, w tym instytucje płatnicze zwolnione zgodnie z dyrektywą (UE) 2015/2366;
- ▶ dostawców świadczących usługę dostępu do informacji o rachunku;
- ▶ instytucji pieniądza elektronicznego, w tym instytucji pieniądza elektronicznego zwolnionych zgodnie z dyrektywą 2009/110/WE;
- ▶ firm inwestycyjnych;
- ▶ centralnych depozytów papierów wartościowych;
- ▶ zewnętrznych dostawców usług ICT²¹¹.

DORA stanowi część wprowadzonego przez UE pakietu aktów prawnych związanych z rozwojem technologicznym. Do Rozporządzenia DORA w 2024 r.

209 Dz.U. UE. L. z 2022 r. Nr 333, str. 1

210 Dz.U. UE. L. z 2022 r. Nr 333, str. 80

211 Zob. pozostałe podmioty wymienione w art. 2 DORA. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022R2554>, dostęp: 2 stycznia 2024 r.

208 Dz.U. UE. L. z 2023 r. poz. 2854.

mają zostać wydane akty wykonawcze, które będą determinowały dokładne ramy wymogów, które adresaci DORY będą musieli wypełnić.

Zaznaczyć należy, że DORA będzie obejmować następujące obszary:

- ▶ zarządzanie ryzykiem ICT;
- ▶ zgłaszanie incydentów ICT przez podmioty finansowe zarówno na poziomie krajowym jak i europejskim;
- ▶ testowanie operacyjnej odporności cyfrowej;
- ▶ zarządzanie ryzykiem dostawców usług ICT;
- ▶ określenie ram kontroli i nadzoru krajowych oraz unijnych organów nadzoru – w tym określenie ram dla kluczowych dostawców usług ICT i łańcuchem dostaw.

Celem Dyrektywy NIS 2 jest zapewnienie wysokiego poziomu odpowiedzialności za środki zarządzania ryzykiem w zakresie cyberbezpieczeństwa oraz obowiązki w zakresie zgłaszania incydentów na poziomie podmiotów kluczowych i ważnych. **Dyrektywa NIS 2 w załączniku wskazuje, że podmioty z sektora bankowości oraz infrastruktury rynków finansowych są podmiotami kluczowymi.**

Dyrektywa NIS 2 określa:

- ▶ obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz wyznaczenia lub powołania właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa (pojedyncze punkty kontaktowe) oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT);
- ▶ środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów spoczywające na podmiotach w rodzaju tych, o których mowa w załączniku I lub II, jak również na podmiotach zidentyfikowanych jako podmioty o charakterze krytycznym na podstawie dyrektywy (UE) 2022/2557;
- ▶ zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie;

- ▶ obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.

W art. 21 Dyrektywy NIS 2 ustanowiono środki zarządzania ryzykiem w cyberbezpieczeństwie. Z kolei w artykule 23 Dyrektywy NIS 2 zostały ujęte obowiązki w zakresie zgłaszania incydentów²¹².

Dyrektywa NIS 2 Dyrektywa weszła w życie 16 stycznia 2023 r. Państwa członkowskie muszą przyjąć i opublikować przepisy niezbędne do wykonania dyrektywy do 17 października 2024 r.

[Rozporządzenie w sprawie rynku kryptoaktywów (dalej jako: „MiCA”²¹³)]

Rozwój kryptowalut „wymusił” na UE uregulowanie sektora kryptowalut. W celu dostosowania unijnych aktów ustawodawczych przez UE do epoki cyfrowej. Warto zaznaczyć, że MiCA wzorowana była na dotychczas obowiązujących aktach normatywnych, takich jak MIFID²¹⁴, czy MAR²¹⁵.

Dodać należy, że MiCA w swojej treści wielokrotnie odwołuje się do przepisów przeciwdziałającym praniu brudnych pieniędzy (AML)²¹⁶. Uznać należy, że MiCA zapewnia ochronę konsumentów, wspiera stabilność i odporność profesjonalnych uczestników tego rynku oraz poprawia uczciwość obrotu przy jednoczesnym ograniczeniu ryzyka.

W doktrynie wskazuje się, że: *„Uchwalenie MiCA należy uznać za adekwatną i dopasowaną do prawa unijnego odpowiedź na dynamiczny i globalny rozwój rynku kryptoaktywów. Przyjęte zostało bowiem spójne z unijnym prawem wtórnym podejście „twardej” regulacji, w której przepisy i wymogi nad-*

212 Zgodnie z art. 6 ust. 6 Dyrektywy NIS 2: „incydent” oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2555>, dostęp: 2 stycznia 2024 r.

213 Rozporządzenie 2023/1114 w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937.

214 Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE.

215 Rozporządzenie Parlamentu Europejskiego i Rady nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektyw Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE.

216 R. Bujalski, *UE reguluje rynki kryptoaktywów (MiCA)*, 2023 r., Lex.



zorcze nakierowane są przede wszystkim na zapewnienie stabilności rynkowej oraz ochronę usługobiorców”²¹⁷.

[Wytyczne]

Nie należy tracić z pola widzenia, że wytyczne dotyczące zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT instytucji finansowych zostały określone przez Europejski Urząd Nadzoru Bankowego²¹⁸.

Warto zaznaczyć, że zasadę proporcjonalności oraz zasadę *risk based approach* można odnaleźć w Wytycznych Europejskiego Urzędu Nadzoru Bankowego z dnia 25 lutego 2019 r. (EBA/GL/2019/02) w sprawie outsourcingu czy Komunikatu UKNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z dnia 23 stycznia 2020 r.

W kontekście identyfikacji systemów pod kątem wypełnienia wymogów regulacyjnych, dostrzec należy obowiązującą Rekomendację D dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach²¹⁹. Wedle Rekomendacji 8: „*Bank powinien posiadać sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności, obejmujące w szczególności zarządzanie architekturą oraz jakością danych i zapewniające właściwe wsparcie działalności banku*”.

Odnotować również należy, że UKNF we wrześniu 2023 r. wydał Stanowisko dotyczące prawidłowego wykorzystania w sektorze finansowym rozwiązań w zakresie nawiązywania stosunków gospo-

darczych bez fizycznej obecności klienta²²⁰. Co istotne, Stanowisko UKNF zawiera dobre praktyki dotyczące realizacji obowiązków wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu²²¹ oraz uwzględnia wytyczne EBA dotyczące wykorzystania rozwiązań w zakresie zdalnego nawiązywania relacji z klientami na podstawie art. 13 ust. 1 dyrektywy (UE) 2015/849 (EBA/GL/2022/15 z dnia 22 listopada 2022 r.), wydane na podstawie art. 16 rozporządzenia (UE) nr 1093/2010, w odniesieniu do przepisów prawa polskiego i ram regulacyjnych dotyczących zapobiegania praniu pieniędzy i finansowaniu terroryzmu.

W zakresie podejmowanej tematyki zasadnym jest również odwołanie się do stanowiska UKNF w sprawie świadczenia usługi robo-doradztwa z dnia 4 listopada 2020 r.²²². Uznać należy, że w świetle procedowanego AI ACT treść stanowiska UKNF może ulec znacznemu zdezaktualizowaniu.

Nie sposób również nie wspomnieć o Rekomendacji W²²³ dotyczącej zarządzania ryzykiem modeli w bankach oraz Rekomendacji J²²⁴, która dotyczy zasad gromadzenia i przetwarzania przez banki danych o nieruchomościach.

Należy także mieć na względzie Komunikat UKNF z dnia 23 stycznia 2020 r. dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze

217 K. Stolarski, *Wpływ MiCA na regulacyjnoprawne uwarunkowania prowadzenia działalności z wykorzystaniem kryptoaktywów w Polsce i UE*, „Monitor Prawniczy”, 9/2023, Legalis.

218 Wytyczne EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT, EBA/GL/2019/04, EBA, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880823/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_PL.pdf dostęp: 10 marca 2024 r.

219 Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, KNF, styczeń 2013, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf

220 Stanowisko UKNF dotyczące prawidłowego wykorzystania w sektorze finansowym rozwiązań w zakresie nawiązywania stosunków gospodarczych bez fizycznej obecności klienta wrzesień 2023 r. https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_prawidlowego_wykorzystania_w_sektorze_finansowym_rozwiazan_w_zakresie_nawiazywania_stosunkow_gospodarczych_bez_fizycznej_obecnosci_klienta_84094.pdf, dostęp: 2 stycznia 2024 r.

221 Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. z 2023 r. poz. 1124.

222 Stanowisko UKNF z dnia 4 listopada 2020 r. w sprawie świadczenia usługi robo-doradztwa, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_swiadczenia_uslugi_robo_doradztwa_71303.pdf, dostęp: 3 stycznia 2024 r.

223 Rekomendacja W dotycząca zarządzania ryzykiem modeli w bankach, KNF, lipiec 2015, https://www.knf.gov.pl/knf/pl/komponenty/img/knf_137749_Rekomendacja_W_42219.pdf, dostęp: 3 stycznia 2024 r.

224 Rekomendacja J dotycząca zasad gromadzenia i przetwarzania przez banki danych o rynku nieruchomości, KNF, marzec 2023, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_J_2023_81609.pdf (dostęp: 3 stycznia 2024 r.



obliczeniowej publicznej lub hybrydowej²²⁵. Wskazane w komunikacie wymogi – stanowią uzupełnienie zaleceń w zakresie outsourcingu, opisanych między innymi w Rekomendacji D oraz PB.

Na sektor bankowy stosowne obowiązki prawne nakładają również Wytyczne EBA w sprawie outsourcingu (EBA/GL/2019/02)²²⁶ jak i stanowisko UKNF dotyczące wybranych zagadnień związanych z wejściem w życie wytycznych EBA²²⁷.

W kontekście przywołanych Wytycznych EBA ws, outsourcingu warto dodać, że we wrześniu 2023 r. znowelizowano PB. Nowelizacja ustawy miała na celu dostosowanie krajowej regulacji do Wytycznych EBA/GL/2019/02.

W uzasadnieniu projektu ustawy wskazano: „W związku z powyższym projekt przewiduje,

w art. 6db ust. 1 ustawy – Prawo bankowe, że w przypadku powierzenia czynności pomiędzy bankiem hipotecznym a bankiem krajowym, który jest jedynym akcjonariuszem, nie ma zastosowania art. 6a ust. 3 ustawy – Prawo bankowe. W konsekwencji rozszerzenia dopuszczalnego zakresu przedmiotowego outsourcingu pokrywającego się z zakresem określonym w Wytycznych EBA, możliwy byłby outsourcing większości funkcji banku (tj. procesów, usług i działań) przy zachowaniu podziału funkcji na krytyczne lub istotne oraz pozostałe, co umożliwi outsourcingowanie m.in. części funkcji zarządzania ryzykiem w ramach grupy kapitałowej”²²⁸.

Po zmianach PB: (i) rozszerza możliwości powierzenia czynności w odniesieniu do umów o instrumenty płatnicze, inne niż karty płatnicze, (np. pieniądź elektroniczny); (ii) dopuszcza możliwość podoutsourceingu w szerokim zakresie.

225 Komunikat UKNF z dnia 23 stycznia 2023 r. dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf, dostęp: 3 stycznia 2024 r.

226 Wytyczne w sprawie outsourcingu, EBA/GL/2019/02, EBA, 25.02.2019 r., https://extranet.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/7551b1c5-534d-44aa-b524-61eb8929154d/EBA%20revised%20Guidelines%20on%20outsourcing_PL.pdf?retry=1, dostęp: 3 stycznia 2024 r.

227 Stanowisko UKNF dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnianiem w działalności banków, UKNF, 16.09.2019 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Stnowisko_UKNF_ws_outsourcingu_67075.pdf, dostęp: 3 stycznia 2024 r.

228 Uzasadnienie do projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku dostępne na stronie internetowej Rządowego Centrum Legislacji, s. 20-21, <https://legislacja.rcl.gov.pl/docs//2/12372806/12976931/dokument625583.pdf>, dostęp: 3 stycznia 2024 r.

5. Podsumowanie wyników badań





Jak ustalono w trakcie wywiadów przeprowadzonych z respondentami:

- ▶ wszyscy respondenci podkreślali konieczność ścisłej współpracy pracowników banku odpowiedzialnych za sferę prawną i otoczenie regulacyjne (w tym compliance) ze specjalistami od technologii;
- ▶ reprezentanci polskiego sektora bankowego świadomi są wyzwania interdyscyplinarności, w tym zwłaszcza integracji perspektywy prawniczej z wiedzą technologiczną, związanego ze stosowaniem sztucznej inteligencji;
- ▶ we wszystkich przeprowadzonych wywiadach akcentowano nie tylko najwyższą troskę o jakość wykorzystywanych mechanizmów bazujących na sztucznej inteligencji, jak i przekonanie, że pozostają one w zgodzie z obowiązującym prawem;
- ▶ sygnalizowano wręcz, że – w razie wystąpienia najmniejszych choćby wątpliwości lub zastrzeżeń co do ich legalności – banki, jako instytucje zaufania społecznego oraz jedne z najściślej regulowanych przedsiębiorców, minimalizują ryzyko, unikając stosowania danego rozwiązania (lub stosując je w ramach testów wewnętrznych, pilotaży, symulacji lub „zabaw” albo wyłącznie pomocniczo i pod ścisłym nadzorem człowieka);
- ▶ zmiany stanu prawnego – zarówno otoczenia legislacyjnego, jak i wykładni prawa, prezentowanej w rozstrzygnięciach sądów, organów lub choćby stanowiskach instytucji publicznych (np. Komisji Nadzoru Finansowego) – charakteryzowane są jako jedna z największych potencjalnych przeszkód lub wręcz ryzyk związanych z zastosowaniem sztucznej inteligencji;
- ▶ zdecydowana większość uczestników rozmów widzi sztuczną inteligencję jako szansę wsparcia i udoskonalenia dotychczasowych (tradycyjnych) procedur, w których kluczową rolę odgrywa realny człowiek. Podkreśla się tu m.in. szybkość prowadzonych operacji, oszczędność zasobów, permanentną dostępność tej technologii oraz możliwość jednoczesnej obsługi wielu klientów naraz;
- ▶ podkreślano, że obecnie możliwości oferowane przez sztuczną inteligencję są testowane i wery-

fikowane jako alternatywne względem dotychczasowych procedur, w których główną rolę odgrywał człowiek;

- ▶ kilkukrotnie wybrzmiało przekonanie, że niejednokrotnie nieprawidłowa prognoza sztucznej inteligencji spowodowana jest błędem ludzkim, efektem zaniedbań, popełnionych na wcześniejszym etapie, polegających przykładowo na wprowadzeniu niepełnych lub niewłaściwych danych;
- ▶ potwierdzono, że AI pełni aktualnie jedynie „rolę wspierającą” procesy decyzyjne, nie zastępując, czy tym bardziej nie eliminując czynnika ludzkiego, a już z pewnością nie uchylając nadzoru pełnionego przez pracowników banku;
- ▶ technologie oparte na AI służą m.in. udoskonaleniu procesu ewaluacji jakości usług oraz wykorzystaniu jej do identyfikacji mankamentów i podniesienia ich poziomu w przyszłości;
- ▶ respondenci mają świadomość towarzyszącym sztucznej inteligencji obawom ze strony pracowników, zaniepokojonych zmianami na rynku pracy oraz nowoczesnymi technologiami, które w niedalekiej przyszłości zdolne będą zastąpić część personelu, prowadząc do redukcji etatów;
- ▶ uczestnicy badania są raczej zgodni w kwestii zmiany obejmującej profil pożądanych pracowników oraz charakter wykonywanej przez nich pracy, która przesunie się bardziej na nadzór nad narzędziami sztucznej inteligencji;
- ▶ wszyscy respondenci deklarują działalność edukacyjną na polu sztucznej inteligencji, skierowaną w pierwszej kolejności do pracowników banku, lecz również osób zewnętrznych, w tym konsumentów, klientów biznesowych, a nawet obywateli i przedsiębiorców niebędących klientami banku;
- ▶ akcentowany jest dystans, krytycyzm i ostrożność w aplikowaniu rozwiązań opartych na AI, co jest w stanie dać najlepszy efekt, równoważąc zalety z wadami i potencjalnymi ryzykami;
- ▶ jednocześnie respondenci podkreślają potencjalne bardzo szerokie i różnorodne pola zastosowania AI przez banki;



- ▶ czy zastosowanie sztucznej inteligencji w bankowości oznaczać będzie raczej stopniową ewolucję, czy jednak radykalną rewolucję w funkcjonowaniu banków, które były znane dotychczas – większość respondentów wskazało na ewolucję;
- ▶ respondenci są świadomi powagi zmian w otoczeniu prawno-regulacyjnym, związanym z AI ACT;
- ▶ niemal wszyscy respondenci bardzo wysoko oceniają poziom zaawansowania technologicznego polskiego sektora bankowego, wskazując krajowe banki jako liderów na tle innych państw Unii Europejskiej;
- ▶ respondenci deklarują przyjmowanie przez ich banki postawy proaktywnej, mającej na celu minimalizację wszelkich ryzyk oraz eliminację rozwiązań potencjalnie niebezpiecznych, bo wątpliwych prawnie;
- ▶ respondenci zdają się trafnie identyfikować największe związane z nim zagrożenia i ryzyka, a nawet intuicyjnie wyczuwać rozwiązania wrażliwe, potencjalnie problematyczne, narażające bank na sankcje, kary, roszczenia odszkodowawcze (m.in. dotyczące naruszania przepisów o danych osobowych, zbierające i wykorzystujące niektóre wrażliwe dane biometryczne, badające zdolność kredytową z potencjalnym naruszeniem obowiązujących zasad, w tym wyjaśnialności);
- ▶ jednym z najpoważniejszych wyzwań towarzyszących prawodawcy dążącemu do uregulowania sztucznej inteligencji, będzie już samo jej legalne zdefiniowanie;
- ▶ ograniczonym entuzjazmem cieszy się koncepcja samoregulacji sektora bankowego w zakresie AI; reprezentanci sektora bankowego – mający świadomość ryzyk związanych ze sztuczną inteligencją oraz przyzwyczajeni do „twardych” wymogów, wynikających z prawa powszechnie obowiązującego – preferują raczej konkretne i precyzyjne ramy ustawowe niż normy mające oparcie w kodeksach etyki, dobrych praktyk, czy ogólnych wytycznych;
- ▶ sformułowano obawę przed „przeregulowaniem” nowoczesnych technologii, w tym AI, w prawie unijnym, które – inaczej niż kraje azjatyckie lub USA – niekiedy przesadnie chroni konsumenta

usług bankowych, ograniczając w ten sposób postęp technologiczny sektora bankowego;

- ▶ respondenci są świadomi faktu, iż AI ACT nie dostarczy odpowiedzi na wszystkie pytania i wątpliwości prawne, otwierając zarazem drogę do dalszych, bardziej szczegółowych regulacji na poziomie krajowym.

Jak wykazała ponadto analiza bazująca na dokumentach dostępnych w domenie publicznej:

- ▶ polskie banki są bardzo aktywne na obszarze popularyzacji sztucznej inteligencji i nowych technologii, pełniąc zarazem ważną funkcję rozwojową oraz edukacyjną (a zatem ogólnospołeczną);
- ▶ poza jej promowaniem, „oswajają” w ten sposób użytkowników z rozwiązaniami AI;
- ▶ akcje takie są zarazem okazją do popularyzacji pożądanых postaw dotyczących nie tylko indywidualnego życia poszczególnych osób (np. oszczędność, planowanie przyszłości, zdrowy tryb życia czy decyzje emerytalne), lecz również ważnych spraw ogólnospołecznych – jak np. zrównoważony rozwój, ekologia, tolerancja, bezpieczeństwo w ruchu drogowym, partycypacja społeczna, empatia;
- ▶ potwierdzenie znalazła teza, iż aktualnie polskie banki są nie tylko typowymi przedsiębiorstwami finansowymi, ale zarazem potężnymi i prężnie rozwijającymi się firmami technologicznymi, zatrudniającymi dziesiątki specjalistów z branży IT;
- ▶ polskie banki mogą być nie tylko ocenione jako nowatorskie i zaangażowane technologicznie, ale – choć wdrażają je z ostrożnością i wyłącznie pod nadzorem czynnika ludzkiego – wykorzystują lub próbują wykorzystywać (poprzez testy) rozwiązania bazujące na sztucznej inteligencji praktycznie we wszystkich możliwych obszarach, w tym służące zarówno wsparciu *front office*, jak i *back office*.
- ▶ nawet obecnie – mimo faktycznej deregulacji licznych obszarów związanych z AI – osoby decyzyjne w bankach trafnie identyfikują ryzyka, unikając takich zastosowań AI, które mogłyby wchodzić w konflikt z prawami człowieka i indywidualnymi wolnościami, a także zapobiegać dyskryminacji, stronnictwu, a zapewniać wyjaśnialność i przejrzystość tych narzędzi.



Jak wynika z przeprowadzonej analizy komparatywnej (prawnoporównawczej):

- ▶ do zasadniczych wyzwań, dotyczących w równym stopniu wszystkich omówionych porządków prawnych, związanych ze stanowieniem prawa w obszarze nowych technologii z całą pewnością należy kwestia skonstruowania definicji legalnej pojęcia „sztuczna inteligencja”;
- ▶ doświadczenia zagraniczne potwierdzają przypuszczenie, iż wraz z reorganizacją modelu świadczenia usług bankowych, część pracowników zostaje zwolniona lub przeniesiona na inne stanowiska;
- ▶ coraz szersze wykorzystanie rozwiązań opartych na SI wymaga posiadania przez pracowników określonych kompetencji, takich jak szybkość reakcji czy zdolność adaptacji, oraz umiejętności, jak np. automatyzacja pracy biurowej i (przynajmniej podstawowych) kompetencje z zakresu informatyki;
- ▶ korzystne wydaje się nawiązanie współpracy z uniwersytetami lub instytucjami badawczymi dysponującymi niezbędną w tym zakresie wiedzą, która pozwoli nie tylko na stworzenie odpowiednich dla sektora bankowego rozwiązań opartych na systemach sztucznej inteligencji, ale również przeszkolenie pracowników z właściwego ich użycia oraz przygotowanie instrukcji dla klientów;
- ▶ występują poważne (fundamentalne) różnice w podejściu do stanowienia prawa sztucznej inteligencji w odmiennych kulturach i tradycjach prawnych, uzależnione również od panującego systemu politycznego;
- ▶ najistotniejszym uniwersalnym wyzwaniem wydaje się kwestia zapobiegania dyskryminacji automatycznej, zapewnienie bezpieczeństwa, ochrona danych osobowych, informowanie użytkowników o zastosowaniu AI oraz ustalenie cech godnego zaufania systemu SI;
- ▶ niezależnie od partykularnych rozwiązań prawnych, zaleca się stały nadzór (zarówno przez pracowników banku, jak i aktywność państwowych organów nadzoru) nad treściami generowanymi przez SI i zapewnienie możliwości następcej ingerencji w model SI;

- ▶ pożądanym rozwiązaniem są programy grantowe – finansowane zarówno przez państwo, jak i podmioty prywatne (w tym podmioty sektora bankowego) – w ramach których finansowana będzie działalność rozwojowa AI;
- ▶ sugerowane jest dalsze prowadzenie przez banki działań edukacyjnych w obszarze sztucznej inteligencji, zarówno skierowanych wobec pracowników, jak i osób zewnętrznych, w tym konsumentów, klientów, obywateli.

Analiza aktualnego brzmienia AI ACT prowadzi do wniosku, że:

- ▶ tekst aktu permanentnie i znacznie ewoluuje, co utrudnia przygotowanie się adresatów do jego wymogów;
- ▶ niepewność w ustaleniu finalnego brzmienia AI ACT potwierdza obawy, zgodnie z którymi AI należy do zagadnień trudno regulowanych legislacyjnie;
- ▶ jednym z największych wyzwań jest stworzenie definicji legalnej sztucznej inteligencji;
- ▶ regulacja budzi wątpliwości z powodu zbyt krótkiej *vacatio legis*;
- ▶ nieuniknione wydają się być problemy interpretacyjne, które będą musiały być następnie ograniczane nowelizacjami, stanowiskami organów unijnych i krajowych lub orzecznictwem sądowym;
- ▶ niektóre z systemów stosowanych przez banki (zwłaszcza dotyczące biometrii oraz oceny zdolności kredytowej) mają charakter wysokiego ryzyka, co generuje dodatkowe obowiązki oraz ryzyka;
- ▶ banki mogą zostać zakwalifikowane jako dostawca lub podmiot stosujący AI, co z kolei implikuje realizację odpowiednich obowiązków określonych w AI ACT;
- ▶ banki będą musiały powołać odpowiednie zespoły, które zidentyfikują ryzyka oraz dostosują wewnętrzne procedury do AI ACT;
- ▶ AI ACT zawiera szereg obowiązków i wymogów regulacyjnych w szczególności w zakresie ryzyka, w konsekwencji podmioty rynku finansowe-



go oraz podmioty, które świadczą na rzecz instytucji finansowych swoje usługi technologiczne (Fintech, RegTech) będą musiały spełnić nadchodzące wymogi regulacyjne;

- ▶ obecność człowieka w pętli decyzyjnej ma kluczowe znaczenie dla poziomu zaufania społeczeństwa do AI;
- ▶ podmioty stosujące systemy AI wysokiego ryzyka zobligowane są zapewnić nadzór ze strony człowieka nad systemami wysokiego ryzyka;

- ▶ uregulowany jednoznacznie zostanie obowiązek poinformowania osoby fizycznej w odpowiednim czasie, w jasny i zrozumiały sposób o tym, że prowadzi ona interakcję z systemem sztucznej inteligencji;
- ▶ art. 70 AI ACT wymaga od każdego państwa członkowskiego wyznaczenia organu notyfikującego oraz organu nadzoru rynku;
- ▶ AI ACT przewiduje restrykcyjne sankcje za naruszenia.

Załącznik: scenariusz wywiadu z respondentami.



SCENARIUSZ WYWIADU POGŁĘBIONEGO W RAMACH BADANIA PT. „AKTUALNE WYZWANIA PRAWNE ZWIĄZANE Z ZASTOSOWANIEM SZTUCZNEJ INTELIGENCJI W POLSKIM SEKTORZE BANKOWYM”

1. Wprowadzenie (szacowany czas: ok. 5 minut)

- a) Przedstawienie się ankietera.
- b) Opis badań (skład zespołu badawczego, cel badań, metody badań, cel wywiadu pogłębianego, podmiot finansujący badania: Warszawski Instytut Bankowości, sposób popularyzacji wyników badań: raport popularno-naukowy dostępny *open access online*).
- c) Zgoda na rejestrowanie wypowiedzi i wykorzystanie ich wybranych fragmentów w tekście raportu.
- d) Ewentualne dodatkowe pytania do ankietera.

2. Sylwetka Respondenta (ok. 5 minut).

- a) Proszę krótko (w kilku zdaniach, koncentrując się na pełnionych funkcjach, wykonywanych obowiązkach, latach doświadczenia, zrealizowanych projektach) opowiedzieć o swoich doświadczeniach zawodowych związanych z sektorem bankowym.
- b) Proszę ogólnie (w kilku zdaniach, skupiając się zwłaszcza na: pełnionych funkcjach, wykonywanych zadaniach, wykształceniu i ukończonych kursach itp.) opisać swoje doświadczenia w zakresie zastosowania/wdrażania sztucznej inteligencji w sektorze bankowym.

3. Pytania główne – otwarte (ok. 20–30 minut)

- a) Czy i w jaki sposób reprezentowana przez Panią/Pana instytucja (bank, inne przedsiębiorstwo, urząd) wykorzystuje sztuczną inteligencję: proszę podać przykłady zastosowania, dotychczasowe doświadczenia, planowane lub realizowane programy pilotażowe itp.? [swobodna wypowiedź]
- b) Jakie dostrzega Pani/Pan zalety i zagrożenia wynikające z zastosowania sztucznej inteligencji w Pana instytucji / sektorze bankowym? Proszę wskazać przynajmniej jedną za-

letę oraz przynajmniej jedną wadę/zagrożenie. [swobodna wypowiedź].

- c) Czy zastosowanie sztucznej inteligencji zrewolucjonizuje w bankowość/system bankowy w okresie najbliższych dwóch dekad – a jeśli tak, to w jakim kierunku? Proszę o uzasadnienie. [swobodna wypowiedź].
- d) Czy – w związku z dokonującym się postępem technologicznym, coraz szerszym wykorzystaniem nowoczesnych technologii, w tym sztucznej inteligencji oraz związane z tym wyzwania – dostrzega Pani/Pan konkretne działania, które powinien podjąć polski sektor bankowy, organy państwowe lub banki samodzielnie? Przykładowo: stworzenie kodeksu dobrych praktyk, przyjęcie nowych regulacji prawnych, utworzenie nowej instytucji publicznej lub przypisanie nowych kompetencji organom już istniejącym, wdrożenie specjalnych systemów monitoringu itp.? [swobodna wypowiedź]
- e) Jak ocenia Pani/Pan stopień rozwoju polskiego sektora bankowego, uwzględniając wykorzystanie nowoczesnych technologii (nie tylko sztucznej inteligencji), w porównaniu do innych państw (anglosaskich i Unii Europejskiej)? Czy są Pani/Panu znane konkretne przykłady rozwiązań zagranicznych, które przyjęcie warto rekomendować polskim bankom?
- f) [*pytanie fakultatywne²²⁹] Jak ocenia Pani/Pan aktualny, obowiązujący w Polsce/Unii Europejskiej, stan regulacji prawnej w kontekście zastosowania sztucznej inteligencji w sektorze bankowym? Czy jest Pani/Pan w stanie przedstawić ewentualne kierunki lub konkretne propozycje zmian legislacyjnych? [swobodna wypowiedź].

4. Zamknięcie i podsumowanie wywiadu

Czy – poza poruszonymi zagadnieniami i odpowiedziami na dotychczas zadane pytania – widzi Pani/Pan inne istotne kwestie, które warto wskazać?

229 Skierowane do respondentów, którzy wyrażą zgodę na pytania dotyczące zagadnień prawnych.



PROGRAM
ANALITYCZNO
BADAWCZY



Raport przygotowany na zlecenie
Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości