

Kamil Szpyt*

ORCID: 0000-0002-2307-8789

Odpowiedzialność cywilna za szkody wyrządzone klientom w wyniku zastosowania systemów sztucznej inteligencji w działalności bankowej¹

Streszczenie

Artykuł omawia kluczowe zagadnienia związane z odpowiedzialnością cywilną banków za szkody wyrządzone klientom w wyniku zastosowania systemów sztucznej inteligencji (AI). W obliczu dynamicznego rozwoju technologii i rosnącego znaczenia AI w sektorze finansowym tradycyjne zasady odpowiedzialności cywilnej mogą okazać się niewystarczające. Analizowane są problemy związane z identyfikacją podmiotów odpowiedzialnych oraz ocena ryzyka, jakie niesie ze sobą wykorzystywanie zaawansowanych algorytmów. W kontekście braku kompleksowych regulacji prawnych, zarówno na poziomie krajowym, jak i unijnym, artykuł podkreśla potrzebę dogłębnej analizy obowiązujących norm oraz dostosowania ich do nowych wyzwań. Przedstawiono również omówienie wybranych regulacji unijnych, takich jak AI Act oraz projektowane przepisy dotyczące odpowiedzialności za systemy sztucznej inteligencji. Praca koncentruje się na wyzwaniach prawnych związanych z ochroną praw klientów oraz ryzykiem finansowym wynikającym z niewłaściwego lub nieprzewidywalnego działania systemów AI w bankowości.

Słowa kluczowe

sztuczna inteligencja, system sztucznej inteligencji, odpowiedzialność cywilna, delikt, produkt niebezpieczny

1. Wprowadzenie

W dobie dynamicznego rozwoju nowych technologii sztuczna inteligencja (ang. *artificial intelligence*, AI) staje się integralnym elementem działalności coraz większej liczby sektorów gospodarki, w tym również – bankowości². Zastosowanie

* Autor jest doktorem nauk prawnych, adiunktem w Katedrze Prawa Cywilnego Wydziału Prawa, Administracji i Stosunków Międzynarodowych Uniwersytetu Andrzeja Frycza Modrzewskiego.

¹ Badania dofinansowane ze środków przeznaczonych na utrzymanie i rozwój potencjału badawczego w dyscyplinie nauki prawne Nr WSUB/2022/12/00024.

² Wykorzystanie AI w sektorze bankowym to sztandarowy przykład tzw. FinTech, czyli mariażu nowych technologii i działalności bankowej oraz okołobankowej (zob. szerzej o zagadnieniu FinTech: K. Szpyt, *FinTech – pojęcie, historia, rynek*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024, s. 3–20; *idem*, *InsurTech – zarys zjawiska*, [w:] K. Szpyt (red.), *InsurTech. Nowe*

systemów AI w tym ostatnim obszarze przynosi liczne profity, wśród których warto wymienić chociażby zwiększenie efektywności operacyjnej, zmniejszenie kosztów działalności oraz wyższą jakość obsługi klienta³. Niemniej – wraz ze wspomnianymi korzyściami – pojawiają się także nowe wyzwania i zagrożenia, w tym niewystępujące wcześniej ryzyka związane z odpowiedzialnością cywilną za szkody spowodowane przez AI. Problematyka ta zyskuje na znaczeniu zwłaszcza w obliczu braku – na chwilę obecną – szczegółowych regulacji prawnych w tej materii (zarówno na poziomie krajowym, jak i unijnym). Pojawia się też pytanie, czy tradycyjne zasady odpowiedzialności cywilnej, oparte w znacznej mierze na przewidywalności i kontrolowalności działań, nie okażą się w pewnym momencie niewystarczające w kontekście autonomicznych systemów AI, które operują na bazie skomplikowanych algorytmów i dużych zbiorów danych (ang. *Big Data*). Również kwestia wskazania osoby odpowiedzialnej za szkodę staje się o wiele bardziej złożona, gdy uwzględnimy, że przy tworzeniu, udostępnianiu i/lub dystrybuowaniu ww. systemów często dochodzi do współpracy różnych podmiotów, takich jak banki, dostawcy technologii oraz podmioty zajmujące się pozyskiwaniem danych. Jednocześnie bankowość jest sektorem silnie regulowanym, w którym precyzja, zaufanie i bezpieczeństwo odgrywają kluczowe role. Banki w swojej działalności muszą uwzględniać nie tylko potrzebę przestrzegania ogólnych przepisów dotyczących cyberbezpieczeństwa czy ochrony danych osobowych, ale również przepisów sektorowych, dotyczących m.in. zasad ochrony tajemnicy bankowej czy zapobiegania praniu pieniędzy i finansowaniu terroryzmu. To wszystko sprawia, że ewentualne ryzyka naruszeń i nadużyć związanych z zastosowaniem nowych technologii generują w tym przypadku znacznie większe niż zazwyczaj obawy⁴.

technologie w branży ubezpieczeń, Warszawa 2023, s. 7; M. Nowakowski, *FINTECH – technologie, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2020; M. Foltwarski, *Sektor FinTech na europejskim rynku usług bankowych*, Warszawa 2019; W. Szpringer, *Nowe technologie a sektor finansowy. FinTech jako szansa i zagrożenie*, Warszawa 2017).

³ O potencjalnym wzroście dochodów z działalności bankowej związanym z wdrożeniem rozwiązań opartych na sztucznej inteligencji (w tym generatywnej AI) zob. szerzej: V. Kamalnath *et al.*, *Capturing the full value of generative AI in banking* <https://www.mckinsey.com/industries/financial-services/our-insights/capturing-the-full-value-of-generative-ai-in-banking> [dostęp: 15.07.2024]; por. P. Widawski, [w:] *Raport: Sztuczna Inteligencja. Dobre praktyki, aspekty prawne, zastosowanie w sektorze finansowym*, https://fintechpoland.com/wp-content/uploads/2022/03/AI_raport_FIN-1.pdf [dostęp: 15.07.2024]. O innych potencjalnych korzyściach zob. także: J. Grzywacz, E. Jagodzińska-Komar, *Rola sztucznej inteligencji w rozwoju sektora bankowego*, „Nauki Ekonomiczne” 2021, t. 34, s. 22–23.

⁴ G. Bar, *Sztuczna inteligencja i uczenie maszynowe*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym...*, s. 21–22.

Wprowadzenie AI do operacji bankowych każdorazowo wiąże się z koniecznością zrozumienia zarówno potencjalnych wiążących się z tym korzyści, jak i zagrożeń. Nie można zapomnieć, że nawet najbardziej zaawansowane technologie bywają zawodne, a decyzje „podejmowane” przez algorytmy mogą prowadzić do nieprzewidzianych konsekwencji, w tym ogromnych strat finansowych oraz naruszenia praw klientów. Jest to zagadnienie tym istotniejsze, że banki, z uwagi na ich rolę w ochronie powierzonego im kapitału, nieodmiennie kładą duży nacisk na szeroko pojęte zarządzanie ryzykiem i nie należą do podmiotów/instytucji, które w sposób lekkomyślny generowałyby dodatkowo niepotrzebne zagrożenia (mowa tutaj zarówno o ryzyku względem całej swojej działalności, jak i konkretnego klienta)⁵.

Niniejszy artykuł ma na celu analizę problematyki odpowiedzialności cywilnej za szkody wyrządzone klientom⁶ w wyniku zastosowania systemów sztucznej inteligencji *stricto* w działalności samych banków⁷. Z tego względu poza obszarem zainteresowań pozostawiono sytuację wykorzystania ww. systemów przez inne podmioty, które można zaliczyć do szeroko pojętego systemu bankowego, takie jak np. bank centralny, organy nadzorcze, podmioty gwarantujące wypłatę depozytów czy instytucje zrzeszające banki⁸. Podobnie ma się sytuacja ze wszelkiego rodzaju parabankami oraz fintechami, czyli start-upami i spółkami technologicznymi oferującymi usługi okołobankowe w środowisku nowotechnologicznym (należy jednak nad-

⁵ Zob. wywiad przeprowadzony przez A. Prończuk-Omiotek z J. Stryczyńskim (*Jak banki wykorzystują sztuczną inteligencję?*, <https://www.youtube.com/watch?v=bFMZOsh2ADg> [dostęp: 15.05.2024]).

⁶ Pod tym pojęciem na gruncie niniejszego artykułu należy rozumieć każdy podmiot (osobę fizyczną, osobę prawną oraz jednostkę organizacyjną nieposiadającą osobowości prawnej) zawierający z bankiem umowę i korzystający z oferowanych przez niego produktów lub/i usług. Jednocześnie, dla zapewnienia kompleksowości wyводу, w niezbędnym zakresie uwzględniono również sytuację wspomnianych podmiotów na etapie poprzedzającym jeszcze zawarcie umowy, które jednak podejmują w tym celu pewne kontakty z bankiem (np. w celu zweryfikowania ich zdolności kredytowej).

⁷ Na gruncie tego tekstu za obowiązującą zostaje uznana definicja banku zawarta w art. 2 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2023 r. poz. 2488 ze zm.; dalej: pr. bank.). Zgodnie z nią „bank jest osobą prawną utworzoną zgodnie z przepisami ustaw, działającą na podstawie zezwoleń uprawniających do wykonywania czynności bankowych obciążających ryzykiem środki powierzone pod jakimkolwiek tytułem zwrotnym”. Natomiast osoby zainteresowane zapoznaniem się z propozycjami doktryny w zakresie ujęcia wspomnianego terminu powinny sięgnąć do: I. D. Czechowska, *Przegląd definicji banku stanowiącego aktywny kanał dystrybucji produktów ubezpieczeniowych*, „Acta Universitatis Lodzensis. Folia Oeconomica” 2011, nr 259, s. 17–26.

⁸ O polskim systemie bankowym i jego elementach składowych zob. szerzej: M. Zaleska, *Charakterystyka systemu bankowego – uwarunkowania instytucjonalne*, [w:] M. Zaleska (red.), *Współczesna bankowość*, Warszawa 2008, s. 24; A. Iwańczuk, *System bankowy i system płatniczy – powiązania i wzajemne uwarunkowania*, „Zeszyty Naukowe/Akademia Ekonomiczna w Poznaniu” 2008, nr 111, s. 14; T. Ciciрко, K. Kreczmańska-Gigoł, O. Mikołajczyk., M. Mikołajczyk, *Bank centralny i banki komercyjne*, [w:] J. Ostaszewski (red.), *Finanse*, Warszawa 2010, s. 382.

mienić, że zdecydowana większość poczynionych w ramach niniejszego artykułu uwag znajdzie zastosowanie – wprost lub w drodze analogii – również wobec tych podmiotów⁹. Natomiast w celu zapewnienia odpowiedniej kompletności wyводу w opracowaniu w niezbędnym zakresie odniesiono się do ewentualnej odpowiedzialności dostawców rozwiązań technologicznych i innych podmiotów współpracujących z bankami, które potencjalnie mogą odpowiadać za szkody spowodowane przez systemy AI.

W niniejszym tekście skupiono się na cywilnej odpowiedzialności odszkodowawczej, poza zakresem analizy pozostawiając zagadnienia rękojmi i gwarancji¹⁰, obowiązków związanych z dostarczaniem treści i usług cyfrowych¹¹, jak również odpowiedzialności za usterki w oprogramowaniu przewidzianej w przepisach prawa autorskiego¹². Jednocześnie analizie poddano obowiązujące regulacje krajowe i unijne, z uwzględnieniem nieobowiązującego jeszcze rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG)¹³ oraz procedowanego obecnie Wniosku Dyrektywy Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję)¹⁴.

⁹ Na marginesie należy nadmienić, że część przedstawicieli doktryny określa mianem „fintechów” również korzystające z rozwiązań opartych na nowych technologiach banki. Posunięcie to nie wydaje się jednak najlepsze, ponieważ wprowadza niepotrzebne zamieszanie terminologiczne (zob. szerzej: K. Szpyt, *FinTech...*, s. 6).

¹⁰ O problematyce reklamacji i gwarancji w kontekście oprogramowania w czasach sztucznej inteligencji zob. szerzej: A. Michalak, *Odpowiedzialność cywilnoprawna w obrocie oprogramowaniem komputerowym w erze sztucznej inteligencji*, Warszawa 2021, *passim*.

¹¹ Wspomniane obowiązki zostały uregulowane w ustawie z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz. U. z 2023 r. poz. 2759) i wykraczają dalece poza materię odszkodowawczą.

¹² Zob. art. 55 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2022 r. poz. 2509).

¹³ PE/24/2024/REV/1; dalej jako: AI Act.

¹⁴ Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję) (Tekst mający znaczenie dla EOG) {SEC(2022) 344 final} - {SWD(2022) 318 final} - {SWD(2022) 319 final} {SWD(2022) 320 final}, Bruksela 2022 r. COM(2022) 496 final 2022/0303 (COD); dalej jako: projekt dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję.

2. Pojęcie sztucznej inteligencji i systemów sztucznej inteligencji

Skonstruowanie definicji sztucznej inteligencji, nierodzącej zacieklejczych sporów w doktrynie oraz nieobarczonej ryzykiem rychłej dezaktualizacji, stanowiło wyzwanie, z którym od kilku lat próbowano zmierzyć się zarówno w piśmiennictwie, jak i w ramach ustawodawstwa unijnego¹⁵. Pomimo tego liczba nadal istniejących wątpliwości (niejednokrotnie – o niezwykle zniuansowanym charakterze) oraz nagromadzenie literatury przedmiotu sprawiają, że z powodzeniem zagadnienie to mogłoby się stać przedmiotem nie tylko odrębnego artykułu, ale wręcz monografii. Ponieważ jego kompleksowe zgłębianie dalece wykraczałoby poza ramy niniejszego opracowania, wspomniana kwestia zostanie przedstawiona tutaj jedynie w niezbędnym, najistotniejszym zakresie. Dokonując pewnego uproszczenia, można wskazać na dwa podstawowe sposoby rozumienia pojęcia sztucznej inteligencji, a mianowicie jako:

- a) dziedziny wiedzy¹⁶,
- b) systemów maszynowych/programów komputerowych w mniejszym lub większym stopniu starających się imitować ludzki sposób myślenia.

Pierwszy z nich już na pierwszy rzut oka wydaje się nieprzydatny w kontekście dość mocno praktycznych rozważań prowadzonych w niniejszym artykule. Ponadto za wyborem drugiego przemawia fakt, że to do niego sięgnął ustawodawca unijny już przy swoich pierwszych próbach zdefiniowania sztucznej inteligencji. Zostały one podjęte w 2018 r. To wówczas Komisja Europejska wydała Komunikat „Sztuczna inteligencja dla Europy”, zgodnie z którym termin ten „odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowania działań – do pewnego stopnia autonomicznie – w celu osiągnięcia konkretnych celów. Systemy SI mogą być oparte na oprogramowaniu, działając w świecie wirtualnym (np. asystenci głosowi, oprogramowanie do analizy obszaru, wyszukiwarki, systemy rozpoznawania mowy i twarzy), lub mogą być wbudowane w urządzenia (np. zaawansowane roboty, samochody, drony lub aplikacje internetu rzeczy)”¹⁷. Ko-

¹⁵ Szerzej o problemie z właściwym zdefiniowaniem sztucznej inteligencji zob. P. Staszczuk, *Czy unijna regulacja odpowiedzialności cywilnej za sztuczną inteligencję jest potrzebna?*, „Europejski Przegląd Sądowy” 2022, nr 6, s. 25.

¹⁶ Zob. B. Michałowski, A. Przeglasińska, A. Poniewierski, *Internet of Things (IoT) i Artificial Intelligence (AI) w Polsce. Jak wykorzystać rewolucję technologiczną Internetu Rzeczy i Sztucznej Inteligencji w rozwoju Polski. Raport*, Warszawa 2018, <https://sobieski.org.pl/wp-content/uploads/Raport-Iot-i-AI-w-Polsce-03-2018-Micha%C5%82owski.pdf> [dostęp: 15.07.2024], s. 12.

¹⁷ Komunikat z 25.04.2018 r. Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy”, COM/2018/237 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CE->

lejne propozycje definicji pojawiły się m.in. w dokumencie „Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania”¹⁸, w którym Komisja Europejska stwierdziła ogólnie, że „sztuczna inteligencja to zbiór technologii łączących dane, algorytmy i moc obliczeniową”.

Żadna z powyższych definicji nie zyskała jednak powszechnej akceptacji doktryny, w wyniku czego w literaturze przedmiotu – tak polskiej, jak i zagranicznej – zaczęto wysuwać kolejne propozycje ujęcia wspomnianego zagadnienia. Jedną z ciekawszych wysunął T. Zalewski, zdaniem którego „sztuczna inteligencja to system, który pozwala na wykonywanie zadań wymagających procesu uczenia się i uwzględniania nowych okoliczności w toku rozwiązywania danego problemu i który może w różnym stopniu – w zależności od konfiguracji – działać autonomicznie oraz wchodzić w interakcje z otoczeniem”¹⁹.

Wydaje się jednak, że obecnie stan ten ulegnie istotnej zmianie. Przyjęcie przez Parlament Europejski AI Actu wraz z zawartą w nim definicją systemu sztucznej inteligencji na dłuższy czas zdominuje sposób rozumienia rzeczzonego pojęcia w dyskursie prawnym. W szczególności, że do definicji tej odsyła projekt dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję, a i z analogicznym rozwiązaniem niewątpliwie zetkniemy się w przypadku ustawy wdrażającej rozwiązania AI Act w Polsce (mało bowiem prawdopodobne, by polski ustawodawca zdecydował się na zaproponowanie własnej, konkurencyjnej definicji).

Ustawodawca unijny zrezygnował w tym przypadku z prób definiowania samej „sztucznej inteligencji”²⁰, najprawdopodobniej chcąc m.in. uniknąć wspomnianych już sporów co do prawidłowości jej ujęcia i decydując się na zaproponowanie rzeczzonej definicji „systemu sztucznej inteligencji”, co sygnalizuje przesunięcie jego

LEX%3A52018DC0237 [dostęp: 8.05.2024]; do definicji zawartej w tym komunikacie odnosi się i rozwija ją działająca przy Komisji Europejskiej Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji w swoim dokumencie pt. *A Definition of AI: Main Capabilities and Disciplines* (https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf) [dostęp: 15.07.2024].

¹⁸ COM(2020) 65 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020DC0065> [dostęp: 15.07.2024].

¹⁹ T. Zalewski, *Definicja sztucznej inteligencji*, [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, s. 14; zob. także: H. Sheikh, C. Prins, E. Schrijvers, *Mission AI. The New System Technology*, Haga 2023, s. 15 i n.

²⁰ Warto jednak zasygnalizować, że zarówno w dyskursie publicznym, jak i niektórych publikowanych opracowaniach można zaobserwować pewien trend sprowadzający się do dość liberalnego podchodzenia do rozróżnienia pojęć „sztuczna inteligencja” i „system sztucznej inteligencji”, skutkującego wręcz ich synonimicznym stosowaniem. Oczywiście od strony formalnej może to budzić pewne zastrzeżenia. Niemniej, należy pamiętać o tej praktyce zwłaszcza przy okazji analizowania literatury przedmiotu, w której autorzy zdecydowali się na zastosowanie wspomnianego zabiegu.

obszaru zainteresowana z samej technologii na faktyczne przypadki wykorzystania AI w różnych obszarach życia²¹. Z tego też względu również w ramach niniejszego opracowania zdecydowano się na przyjęcie jako wiodącego pojęcia „systemu sztucznej inteligencji”, pod którym – zgodnie z art. 3 pkt 1 AI Act – należy rozumieć: „system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne”.

3. Zastosowanie systemów AI w działalności bankowej

Zgodnie z raportem opracowanym przez Genpact „Commercial banking and the customer experience imperative. How industry leaders are using CX and artificial intelligence to overcome disruption” aż 97% respondentów (w skład których wchodziła kadra kierownicza banków komercyjnych) wskazało na pewien – większy lub mniejszy – poziom wykorzystania sztucznej inteligencji w działalności swoich pracodawców²². Patrząc na to oraz inne badania i doniesienia prasowe, można wysnuć wniosek, że wdrażanie systemów AI w bankowości jest obecnie nie tylko powszechne, ale w wielu przypadkach staje się jednym z priorytetów na najbliższe lata²³. Na gruncie krajowym potwierdzają to zresztą wyniki badań przeprowadzonych przez

²¹ J. Kozłowski, [w:] Law4Tech, *Analiza i ocena zmian w Akcie o sztucznej inteligencji (AI Act)*, <https://law4tech.pl/1881-2/> [dostęp: 15.07.2024]; na wspomnianą kwestię posłużenia się dwoma terminami zwrócili również pośrednio uwagę G. Bar, M. Nowakowski, R. Prabucki i D. Szostek w przygotowanym przez siebie raporcie, nie decydując się jednak na jej dokładniejsze omówienie (*idem*, *Zastosowanie sztucznej inteligencji w bankowości – szanse oraz zagrożenia. Analiza prawno-regulacyjna wpływu technologii uczenia maszynowego i pokrewnych na obowiązki sektora bankowego z zakresu zapewnienia zgodności oraz zarządzania ryzykiem*, s. 7–9, https://us.edu.pl/wp-content/uploads/pliki/PAB_WIB_Zastosowanie_sztucznej_inteligencji_w_bankowosci_Szostek.pdf [dostęp: 15.07.2024]).

²² Genpact, *Commercial banking and the customer experience imperative How industry leaders are using CX and artificial intelligence to overcome disruption*, s. 7, <https://website-files.genpact.com/files/report-commercial-banking-and-the-customer-experience-imperative.pdf> [dostęp: 15.07.2024].

²³ McKinsey, *Global Banking Annual Review 2023: The Great Banking Transition*, <https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review#/> [dostęp: 15.07.2024]; por. Institute for Development and Research in Banking Technology (Established by Reserve Bank of India), *AI in Banking. A Primer*, https://www.idrbit.ac.in/wp-content/uploads/2022/07/AI_2020.pdf [dostęp: 15.07.2024]; por. K. Maj, *Sztuczna inteligencja w prawdziwym banku*, [w:] Związek Banków Polskich, Centrum Prawa Bankowego i Informacji, *Sztuczna inteligencja w bankowości*, Warszawa 2020, s. 10–27, <https://bank.pl/wp-content/uploads/2020/06/Raport-SZTUCZNA-INTELI-GENCJA.pdf> [dostęp: 15.07.2024].

portal [Cashless.pl](https://www.cashless.pl), a dotyczących wykorzystania AI przez banki działające w Polsce. Zgodnie z nimi aż 12 na 13 ankietowanych instytucji ma już za sobą wdrożenie podobnych rozwiązań²⁴.

Dążąc do pewnego uporządkowania powyższej materii, w doktrynie podejmuje się próby pogrupowania systemów AI w bankowości w zależności od obszaru, który wspierają: czy jest to tzw. *front office*, czy też *back office*²⁵. Ten pierwszy obszar odnosi się do wykorzystania wspomnianych rozwiązań w relacjach z podmiotami zewnętrznymi, ten drugi – zastosowania ich do procesów wewnętrznych banku²⁶.

Wspomniany podział, jakkolwiek najpowszechniejszy i pozwalający lepiej zrozumieć specyfikę wdrażania rozwiązań AI w bankowości, nie wydaje się wystarczająco szczegółowy z punktu widzenia podjętej w niniejszym artykule problematyki. W tym kontekście lepiej sprawdzi się nieco bardziej rozbudowana systematyzacja, rozpoczynająca się od wyróżnienia dwóch kategorii:

- a) wykorzystania systemów AI w ramach wewnętrznych zastosowań banku, niebędących działalnością regulowaną (np. w zakresie rekrutacji nowych pracowników),
- b) wykorzystania systemów AI w relacjach z podmiotami trzecimi.

W trym drugim przypadku można dokonać dalszego podziału na następujące grupy:

- a) relacje banku z klientami (obecnymi i przyszłymi),
- b) relacje banku z innymi bankami,
- c) relacje banku z innymi niż banki podmiotami (np. zakłady ubezpieczeń, fintechy),
- d) relacje banku z organami nadzoru.

Jak łatwo się domyślić, przedmiotem naszego zainteresowania będą przede wszystkim działania zaliczane do pierwszej ze wskazanych kategorii. Celowo posłużono się tutaj zwrotem „przede wszystkim”, gdyż prawdopodobne jest wystąpienie sytuacji, w których również w relacjach bank–bank oraz bank–podmiot

²⁴ J. Uryniuk, *Cashless Breakfast AI. Nest Bank zaprezentował bazującego na GPT-4 N!Asystenta*, <https://www.cashless.pl/15110-cashless-breakfast-ai-n-asystent-nest-bank> [dostęp: 15.07.2024].

²⁵ Ailleron, *AI w bankowości – sztuczna inteligencja w banku i finansach*, <https://ailleron.com/pl/baza-wiedzy/ai-w-bankowosci-sztuczna-inteligencja-w-banku-i-finansach/> [dostęp: 15.07.2024].

²⁶ W niektórych opracowaniach w ramach wspomnianego podziału wyróżnia się również trzecią grupę, tzw. obszar *middle office*. Na takie rozwiązanie zdecydowali się autorzy raportu „AI in Business and Finance. OECD Business and Finance Outlook 2021” przygotowanego w ramach Organizacji Współpracy Gospodarczej i Rozwoju (ang. Organisation for Economic Cooperation and Development, OECD). Do wspomnianego obszaru zalicza się wówczas m.in. przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu oraz przeciwdziałanie oszustwom (zob. OECD, *AI in Business and Finance. OECD Business and Finance Outlook 2021*, <https://www.oecd-ilibrary.org/docserver/ba682899-en.pdf?expires=1721927852&id=id&accname=guest&checksum=7EFEBE8DF7D760F0216FBD-21CF486116> [dostęp: 15.07.2024]).

trzeci nie będący bankiem może dojść do naruszenia praw klienta i wyrządzenia mu szkody. Przykładowo – poprzez przekazanie jego danych osobowych bez jakiegokolwiek podstawy prawnej. Tym samym przedstawiony podział ma jedynie charakter pomocniczy, pozwalający lepiej zrozumieć omawianą materię oraz wyodrębnić obszary, w których najczęściej będzie dochodziło do wyrządzenia szkody klientowi.

Katalog zastosowań systemów sztucznej inteligencji w relacji bank–klient nie będzie miał charakteru zamkniętego, niemniej wśród najpowszechniejszych z nich należy wymienić:

a) chatboty, voicboty oraz wirtualni asystenci – są to rozwiązania wykorzystywane zarówno na etapie całkowicie przedkontraktowym, jak i w trakcie „rozmów” z obecnymi już klientami i proponowania im nowych produktów oraz usług lub podejmowania prób rozwiązania ich problemów. Zaliczyć do nich należy zarówno powszechne już systemy udzielające odpowiedzi w oparciu o proste drzewka konwersacji, jak i te bardziej rozbudowane, niebazujące na konkretnej ścieżce konwersacji i umożliwiającym komunikowanie się z chatbotem/voicebotem/wirtualnym asystentem przy pomocy języka naturalnego (swobodnej konwersacji)²⁷;

b) aplikacje mobilne i desktopowe;

c) weryfikacja danych identyfikacyjnych klientów, w tym danych biometrycznych – mowa tutaj o ich wykorzystywaniu zarówno do identyfikacji, jak i weryfikacji klientów (w tym m.in. do zakładania kont bankowych oraz potwierdzania płatności)²⁸;

d) rozwiązania usprawniające procesy rozpatrywania reklamacji;

e) rozwiązania wspierające działania o charakterze marketingowym;

f) rozwiązania umożliwiające personalizację produktów oraz wydawanie rekomendacji produktowych;

g) zautomatyzowane systemy doradztwa, w szczególności inwestycyjnego (tzw. robo-doradztwo) – niewątpliwą zaletą wdrożenia systemów AI może być bardzo daleko idąca personalizacja ofert bankowych (hiperpersonalizacja), przy jednocześnie niskim koszcie ich sporządzenia (mówimy tutaj o weryfikowaniu zarówno obecnych, jak i przyszłych potrzeb klientów)²⁹;

²⁷ Jako przykład tego drugiego można wskazać np. bazującego na modelu językowym GPT-4 N!Asystenta wdrożonego przez Nest Bank (J. Uryniuk, *op. cit.*; *Klienci Nest Banku już testują AI Asystenta*, <https://nestbank.pl/n-asystent-juz-jest> [dostęp: 15.07.2024]).

²⁸ Zob. szerzej: M. Sudoł, *Biometria w identyfikacji i weryfikacji klientów bankowych*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym...*, s. 139–147.

²⁹ Zob. szerzej: H. Jankowska, *Robo-doradztwo*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym...*, s. 207–224.

h) systemy oceny zdolności kredytowej oraz ryzyka kredytowego – wykorzystanie systemów sztucznej inteligencji do analizowania zdolności kredytowej i scoringu kredytowego jest jedyną działalnością *stricto* bankową, która została omówiona w AI Act (zagadnienie to zostanie szerzej poruszone w dalszej części artykułu). Mając na względzie fakt, że wydawanie takich decyzji związane jest z dokonaniem analizy olbrzymiej ilości danych, systemy AI wydają się wprost stworzone do podejmowania działań w podobnych sprawach³⁰.

Istotne znaczenie dla ustalenia zakresu i zasad odpowiedzialności banku za szkody spowodowane przez konkretne systemy AI mogą mieć źródło jego pochodzenia i podstawa prawna, w oparciu o którą wspomniana instytucja z niego korzysta. Nie zawsze bowiem podmiotem odpowiedzialnym musi być bank, a może to być np. podmiot trzeci dostarczający konkretny system. W tym zakresie można wymienić trzy podstawowe modele zaopatrywania się przez banki w rozwiązania oparte na systemach AI:

a) bank posiada własny dział technologiczny/laboratorium innowacji, w ramach którego powstają nowe, wdrażane przez niego rozwiązania – w takim przypadku będzie on zazwyczaj posiadał pełnię praw własności intelektualnej (w tym autorskie prawa majątkowe) do danego wytworu, które nabędzie głównie w oparciu o odpowiednie klauzule w umowach o pracę i umowach cywilnoprawnych ze zleceniobiorcami/wykonawcami;

b) bank nabywa prawa do korzystania z rozwiązań stworzonych przez podmioty zewnętrzne (np. fintechy) – w tym przypadku najczęściej bank będzie jedynie licencjobiorcą lub/i usługobiorcą (w przypadku korzystania z systemu w ramach modelu SaaS³¹); rzadko natomiast będzie dochodziło do nabycia przez niego pełni praw (wynika to ze specyfiki modelu biznesowego przyjętego przez dostawcę technologii, któremu o wiele bardziej w takich sytuacjach opłaca się licencjonować produkt wielu podmiotom);

c) bank wybiera zewnętrzny start-up, który wspiera finansowo (a niekiedy nabywa przedsiębiorstwo lub udziały w nim) w zamian za dostęp do konkretnych rozwiązań technologicznych³² – wówczas bank może zarówno posiadać pełnię praw,

³⁰ Katalog w oparciu o: G. Bar, M. Nowakowski, R. Prabucki, D. Szostek, *op. cit.*, s. 16.

³¹ Ang. Software as a Service, oprogramowanie jako usługa; zob. szerzej o prawnych aspektach SaaS: S. Małkowski, *Charakter prawny umowy Software as a Service w polskim systemie prawnym*, „Prawo Mediów Elektronicznych” 2022, nr 4, s. 49–52.

³² Analogiczne modele występują np. przy tworzeniu nowych rozwiązań z zakresu InsurTech (zob. K. Szpyt, *InsurTech...*, s. 12–14).

jak i być jedynie upoważniony do korzystania z technologii (jest to uzależnione od ustalonego pomiędzy stronami modelu współpracy i zawartych umów).

4. Odpowiedzialność cywilnoprawna za szkody spowodowane przez AI w bankowości

4.1 Ryzyka związane z zastosowaniem AI w bankowości i ich przykłady

Przed przejściem do prezentacji konkretnych reżimów i zasad odpowiedzialności warto wskazać najważniejsze i najczęstsze ryzyka związane z zastosowaniem AI w bankowości, które jednocześnie mogą być źródłem szkód dla klientów (większość z nich zostanie szerzej omówiona w dalszej części artykułu):

- a) błędy i awarie systemów AI – ich skutkiem może być m.in. utrata środków pieniężnych klientów lub ich danych;
- b) trudności z przewidywaniem zachowania systemów AI – rezultatem może być np. wprowadzenie klienta w błąd podczas zawierania umowy lub dopuszczenie się zachowań dyskryminacyjnych;
- c) naruszenie prywatności i bezpieczeństwa danych – rezultatem może być np. nieuprawniony dostęp do danych klientów przez osoby trzecie;
- d) nadużycia i oszustwa – mogą one polegać na wykorzystaniu przez bank zakazanych systemów AI w sposób naruszający zarówno indywidualne interesy klientów, jak i zbiorowe interesy konsumentów;
- e) naruszenie cyberbezpieczeństwa – ich wynikiem może być manipulacja danymi w sposób zagrażający w sposób istotny interesom klienta³³.

Oczywiście liczba ryzyk może być znacznie dłuższa, przy czym często nie będą one rodziły szkód o charakterze cywilnoprawnym, a jedynie pewne konsekwencje natury karnoprawnej lub administracyjnej (np. kary pieniężne).

³³ Kwestie szeroko pojętego cyberbezpieczeństwa nie tylko w sektorze bankowym, ale w całym szeroko pojętym sektorze finansowym należą obecnie do tych wzbudzających największe zainteresowanie przedstawicieli branży. Wynika to z faktu uchwalenia rozporządzenia 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) 2016/1011 (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 333/1 z 2022 r.), które wchodzi w życie 17 stycznia 2025 r. Jego celem jest zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych oraz uregulowanie świadczenia usług ICT (ang. Information and Communications Technology, technologie informacyjno-komunikacyjne) na rynku finansowym. Znajdzie ono zastosowanie również w zakresie tworzenia i wdrażania nowych systemów AI.

4.2 Reżimy i podstawy prawne odpowiedzialności cywilnej za szkody spowodowane przez systemy AI

4.2.1 Uwagi ogólne

Zasadniczo w prawie polskim można wyróżnić cztery podstawowe reżimy odpowiedzialności cywilnej:

- a) odpowiedzialność kontraktową,
- b) odpowiedzialność deliktową,
- c) odpowiedzialność za produkt niebezpieczny³⁴,
- d) odpowiedzialność gwarancyjno-repartycyjną.

Ostatnia z nich jest charakterystyczna m.in. dla zakładów ubezpieczeń, których odpowiedzialność w ramach ubezpieczeń odpowiedzialności cywilnej ma charakter akcesoryjny względem sprawcy szkody. Z tego względu nie będzie ona szerzej analizowana w ramach niniejszego artykułu³⁵.

4.2.2 Odpowiedzialność kontraktowa

W Polsce obowiązuje swoboda kontraktowania³⁶, jednakże specyficzny rodzaj działalności banków oraz jej silne uregulowanie sprawiają, że w praktyce będziemy mieli do czynienia z ograniczoną liczbą umów, wśród których warto wymienić przede wszystkim:

- a) umowę rachunku bankowego³⁷,
- b) umowę pożyczki³⁸,
- c) umowę kredytu (konsumpcyjnego, hipotecznego, inwestycyjnego itd.)³⁹,
- d) umowę o prowadzenie rachunku papierów wartościowych⁴⁰,
- e) umowę o prowadzenie rachunku zbiorczego⁴¹,
- f) umowę gwarancji bankowej⁴².

³⁴ Według niektórych przedstawicieli doktryny odpowiedzialność za produkt niebezpieczny jest podkategorią odpowiedzialności deliktowej, z czym jednak nie sposób się zgodzić.

³⁵ O zagadnieniu ubezpieczeń sztucznej inteligencji zob. szerzej: G. Dybała, K. Szpyt, *Ubezpieczenia sztucznej inteligencji*, [w:] K. Szpyt (red.), *InsurTech. Nowe technologie w branży ubezpieczeń*, s. 274–292; D. Smoleń, O. Sokoliński, G. Szarek, *Polisa od sztucznej inteligencji*, „Miesięcznik Ubezpieczeniowy” 2018, nr 10, s. 34–36.

³⁶ Zob. art. 353¹ ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061); dalej jako: k.c.

³⁷ Art. 725–733 k.c.; art. 49–62 pr. bank.

³⁸ Art. 720–724¹ k.c.

³⁹ Art. 68 pr. bank.

⁴⁰ Art. 121 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz. U. z 2024 r. poz. 722); dalej jako: u.o.i.f.

⁴¹ Art. 121a u.o.i.f.

⁴² Art. 81 pr. bank.

Oczywiście mowa w tym przypadku o umowach stanowiących podwalinę nawiązania stosunku prawnego pomiędzy klientem a bankiem. Jednocześnie nie można zapominać, że w przypadku bankowości elektronicznej (w tym także mobilnej) będzie również dochodziło do zawierania dodatkowych umów o świadczenie usług dostępu do aplikacji czy portalu, względnie – akceptacji regulaminu świadczenia takowych usług.

Odpowiedzialność kontraktowa na gruncie prawa polskiego oparta jest na zasadzie winy. Szkoda spowodowana przez kontrahenta musi być rezultatem niewykonania lub nienależytego wykonania zobowiązania⁴³. Należy w tym miejscu zaznaczyć, że wspomniana szkoda może mieć – co do zasady – charakter wyłącznie majątkowy, a w efekcie niedopuszczalne jest dochodzenie zadośćuczynienia w ramach omawianego reżimu⁴⁴. Poszkodowany dłużnik musi ograniczyć swoje roszczenia jedynie do dochodzenia odszkodowania. Wspomnianych roszczeń nie należy utożsamiać z brakiem spełnienia przez dany produkt lub usługę bankową subiektywnych oczekiwań klienta, np. w zakresie szybkości działania lub estetyki interfejsu bankowości mobilnej (o ile oczywiście nie narusza to pewnych minimalnych, obiektywnych kryteriów określonych w umowie).

Odpowiedzialność kontraktowa na pierwszy rzut oka jawi się jako ta, która najczęściej znajdzie zastosowanie w przypadku szkód wyrządzonych klientowi przez bank. Pojawia się jednak pytanie, czy ta sama prawidłowość wystąpi również w przypadku szkód spowodowanych przez systemy AI.

Wykorzystanie systemów sztucznej inteligencji w bankowości może mieć miejsce już na etapie zawierania umowy. Jako przykład należy wskazać wykorzystanie chatbotów, voicebotów oraz wirtualnych asystentów, które nie tylko są w stanie poinformować obecnego lub potencjalnego klienta o konkretnej ofercie banku i odpowiedzieć na jego pytania, ale również – w niedalekiej przyszłości – najprawdopodobniej przeprowadzić przez cały proces wypełniania umowy/rejestracji/zakładania konta. W tym miejscu rodzi się pytanie, co w sytuacji, gdy system AI wprowadzi klienta w błąd co do treści umowy i w wyniku wspomnianego działania ten ostatni zawrze umowę, na którą – mając prawidłowe informacje – by się nie zdecydował?

Prawdopodobieństwo wystąpienia podobnej sytuacji jest o wiele niższe w przypadku systemów AI korzystających z konkretnej, z góry ustalonej ścieżki konwer-

⁴³ Art. 471 k.c.

⁴⁴ Jedynym wyjątkiem w tym zakresie w prawie polskim jest zadośćuczynienie za zmarnowany urlop przewidziane w art. 50 ust. 2 ustawy z dnia 24 listopada 2017 r. o imprezach turystycznych i powiązanych usługach turystycznych (t.j. Dz. U. z 2023 r. poz. 2211).

sacji. Natomiast odnośnie do skorzystania przez bank z bardziej rozbudowanych rozwiązań, stosujących generatywną sztuczną inteligencję oraz zrozumienie języka naturalnego, ryzyko tzw. halucynacji, czyli podawania przez AI nieprawdziwych lub stronniczych odpowiedzi, gwałtownie rośnie⁴⁵. Zjawisko to jest obecnie zauważalne w przypadku wszystkich powszechnie dostępnych systemów AI, w tym – w wypowiedziach tak popularnego ChataGPT⁴⁶. Niekiedy podejmowane są próby zapobiegania podobnym sytuacjom poprzez wpisywanie promptu (słownej komendy) zakazującego systemowi AI podawania błędnych/fałszywych informacji, o ile nie są mu znane prawdziwe. Po pierwsze, jednak podobne próby nie zawsze odniosą zamierzony skutek. Po drugie, wydaje się niedopuszczalne wymaganie od obecnego lub przyszłego klienta banku, żeby znał tę zależność.

Tego typu działania dopuszczonego przez bank do użytku systemu AI, funkcjonującego dodatkowo jako oficjalny „doradca” banku, niewątpliwie mogą zostać uznane za przykład nieuczciwych praktyk rynkowych w rozumieniu art. 4 ustawy z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym⁴⁷ i w efekcie zrodzić roszczenia odszkodowawcze, o których mowa w art. 12 ust. 1 pkt 4 ww. ustawy. Co znamienne, konsekwencją tego może być również stwierdzenie nieważności umowy zawartej z bankiem⁴⁸.

W tym kontekście rodzi się pytanie: czy opatrzenie komunikatora ostrzeżeniem, że treści podane przez chatbota/voicebota/wirtualnego asystenta mogą być niepoprawne i w celu uzyskania wiarygodnej porady konieczne jest skontaktowanie się z „żywym” konsultantem, może zwolnić bank z odpowiedzialności? Wydaje się, że w celu osiągnięcia takiego rezultatu prawnego konieczne byłoby, żeby komunikat wyświetlał się w widocznym miejscu przy każdej próbie skorzystania z pomocy systemu AI. Inna sprawa, że podobne zabiegi w dłuższej perspektywie należałoby uznać za sprzeczne z istotą samej AI jako rozwiązania służącego zastąpieniu ludzi w wykonywaniu niektórych zadań.

Przechodząc dalej, już na etap funkcjonowania umowy z bankiem, należy wskazać, że w przypadku zaistnienia przesłanek do zarzucenia temu ostatniemu niewy-

⁴⁵ O halucynacjach AI zob. szerzej: W. Iszkowski, R. Tadeusiewicz, *Na marginesie dyskusji o sztucznej inteligencji*, „Nauka” 2023, nr 4, s. 55; J. Kreft, M. Boguszewska-Kreft, B. Cyrek, *Halucynacje chatbotów a prawda: główne nurty debaty i ich interpretacje*, „Rocznik Nauk Społecznych” 2024, t. 16, nr 1, s. 169 i n.; z kolei szerzej o istocie generatywnej sztucznej inteligencji i jej zastosowaniu w bankowości zob. M. Nowakowski, *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023, s. 169–173 i 185–186.

⁴⁶ <https://chat.openai.com/> [dostęp: 15.07.2024].

⁴⁷ T.j. Dz. U. z 2023 r. poz. 845.

⁴⁸ Zob. uchwała Sądu Najwyższego z dnia 11 września 2020 r., III CZP 80/19, Legalis nr 2467749.

konania lub nienależytego wykonania umowy związanego z zastosowaniem w niej systemów sztucznej inteligencji, niewątpliwą podstawą do dochodzenia ewentualnych roszczeń będzie art. 471 k.c. Przykładem tego mogą być błędy i awarie dostarczanych przez bank systemów AI, których skutkiem będzie utrata przez klienta środków pieniężnych (nie tyle dokonanie nieautoryzowanej transakcji, co przysłowiowe „zniknięcie” środków).

Przewidzianą w powyższym przepisie odpowiedzialność można przy tym ograniczyć zgodnie z dyspozycją art. 472 k.c. (o ile – oczywiście – ze szczególnego przepisu ustawy albo z czynności prawnej nie wynika nic innego). W kontekście podobnych zabiegów dotyczących systemów sztucznej inteligencji w działalności bankowej w sytuacji, gdy klient ma status konsumenta, nie można zapominać o art. 385³ pkt 2 k.c., który wskazuje, że „w razie wątpliwości uważa się, że niedozwolonymi postanowieniami umownymi są te, które w szczególności: [...] wyłączają lub istotnie ograniczają odpowiedzialność względem konsumenta za niewykonanie lub nienależyte wykonanie zobowiązania”⁴⁹. Wydaje się, że w przypadku wykorzystania systemów AI w tak newralgicznym sektorze podobne wyłączenia mogą być weryfikowane szczególnie skrupulatnie. Dodatkowo należy zgodzić się z A. Michalakiem, że „ukształtowanie limitu odpowiedzialności w umowie wzajemnej w postaci symbolicznej i nieposiadającej wartości rynkowej kwoty, np. 1 zł, stanowi w istocie nie tyle ograniczenie odpowiedzialności, lecz jej całkowite wyłączenie i w konsekwencji jest nieważne jako sprzeczne z istotą (naturą) każdego zobowiązania, a także z art. 473 § 2 KC, zgodnie z którym nieważne jest zastrzeżenie, że dłużnik nie będzie odpowiedzialny za szkodę, którą może wyrządzić wierzycielowi umyślnie”⁵⁰.

Na marginesie należy zaznaczyć, że jakkolwiek wyżej mowa jest o banku, to z praktycznego punktu widzenia klient każdorazowo powinien zweryfikować, czy dostawcą danego konkretnego produktu lub usługi wykorzystującej AI jest faktycznie bank, czy też podmiot trzeci. Przykładowo, w przypadku uzyskiwania dostępu do informacji o rachunku, zlecenia realizacji płatności oraz sprawdzania dostępności środków na koncie bankowym klient może mieć do czynienia tak naprawdę z zewnętrznym dostawcą usług (ang. *third party provider*, TPP)⁵¹. Ustalenie tego faktu

⁴⁹ Zob. szerzej: J.M. Kondek, *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję (uwagi de lege lata i de lege ferenda)*, Warszawa 2021, s. 11, https://iws.gov.pl/wp-content/uploads/2021/08/IWS_Kondek-J.M._Odpowiedzialnosc-odszkodowawcza-za-oprogramowanie-i-sztuczna-inteligencje.pdf [dostęp: 15.07.2024].

⁵⁰ A. Michalak, *op. cit.*, s. 330.

⁵¹ Zob. przepisy Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywę 2002/65/WE,

będzie miało niebagatelne znaczenie dla ustalenia podmiotu odpowiedzialnego. Natomiast nie można mówić o odpowiedzialności kontraktowej względem klienta podmiotu, który dostarcza bankowi konkretne rozwiązania technologiczne, by ten mógł np. podjąć decyzję odnoszącą się bezpośrednio do klienta. Jako przykład można wskazać sytuację, w której pracownik banku, działający w ramach trybu uproszczonego, skorzystał z opartego na systemie AI programu do wyceny nieruchomości, aby w dalszej kolejności ustalić zdolność kredytową klienta w zakresie zaciągnięcia kredytu hipotecznego (zresztą z takich programów mogą korzystać również występujący w podobnych sprawach rzeczoznawcy majątkowi)⁵². Zazwyczaj przebieg podobnej operacji będzie wyglądał następująco: rzeczoznawca/pracownik banku dokonuje oceny stanu nieruchomości, algorytm AI ocenia wartość nieruchomości, a w ten sposób sporządzona wycena jest w dalszej kolejności weryfikowana przez pracownika. Nawet jeżeli dany program popełni tutaj błąd i w efekcie klient nie otrzyma kredytu, o który się ubiega, nie można w tym przypadku mówić o jakiegokolwiek kontraktowej odpowiedzialności odszkodowawczej względem dostawcy, zarówno z uwagi na brak zawarcia umowy pomiędzy klientem a dostawcą oprogramowania, jak i ze względu na weryfikację i zatwierdzenia wyników wygenerowanych przez system AI przez pracownika banku.

Będąc już przy kwestii podmiotu odpowiedzialnego za szkodę, należy wskazać, że w przypadku bardziej zaawansowanych systemów AI w doktrynie niejednokrotnie rozważana była koncepcja przypisania odpowiedzialności samej sztucznej inteligencji. W tym kontekście rodzi się pytanie: czy istniałaby możliwość zwolnienia się przez bank z ewentualnej odpowiedzialności odszkodowawczej za szkody spowodowane przez niedziałanie lub nienależyte działanie systemu AI poprzez wskazanie, że to właśnie sama sztuczna inteligencja powinna ponosić w tym przypadku odpowiedzialność?

Jednym ze źródeł koncepcji przypisania odpowiedzialności za szkody spowodowane przez AI samej sztucznej inteligencji jest niewątpliwie rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki⁵³, w której wezwano Komisję Europejską do zbadania, przeanalizowania i rozważenia „nadania robotom specjalnego

2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 337/35 z 2015 r.).

⁵² E. Wara-Wąsowska, *jak banki wyceniają wartość mieszkania?*, <https://rynekpierwotny.pl/wiadomosci-mieszkaniowe/wycena-wartosci-mieszkania-przez-bank/11153/> [dostęp: 15.07.2024].

⁵³ (2015/2103(INL)) (2018/C 252/25).

statusu prawnego w perspektywie długoterminowej, aby przynajmniej najbardziej rozwiniętym robotom autonomicznym można było nadać status osób elektronicznych odpowiedzialnych za naprawianie wszelkich szkód, jakie mogłyby wyrządzić, oraz ewentualne stosowanie osobowości elektronicznej w przypadkach podejmowania przez roboty autonomicznych decyzji lub ich niezależnych interakcji z osobami trzecimi” (pkt. 59 lit. f)⁵⁴. Należy jednak wskazać, że idea ta została na późniejszym etapie zarzucona przez ustawodawcę unijnego i nie powróciła w dalszych pracach legislacyjnych nad kolejnymi aktami prawnymi.

Niezależnie od powyższego warto podkreślić, że na obecnym etapie brak podstaw prawnych, by – zarówno na gruncie prawa polskiego, jak i europejskiego – systemom sztucznej inteligencji przypisywać podmiotowość prawną, a w dalszej kolejności także odpowiedzialność cywilną za spowodowane ich działaniami szkody⁵⁵. Wydaje się również, że w najbliższym czasie nie zostaną podjęte żadne inicjatywy w celu zmiany tego stanu rzeczy. Notabene, jest to niewątpliwie słuszne posunięcie. Na dziś takowe działania należy bowiem uznać za co najmniej przedwcześnie i mogące doprowadzić do niepotrzebnego rozmycia się odpowiedzialności odszkodowawczej oraz utrudnienia zaspokojenia roszczeń poszkodowanych. W szczególności warto pamiętać, że systemy AI na obecną chwilę w zasadzie nigdy nie będą dysponować odrębnym majątkiem (zgromadzonym na skutek pracy, dziedziczenia, darowizn itd.), z którego ewentualny poszkodowany mógłby uzyskać zaspokojenie. Pewnym rozwiązaniem byłoby tutaj wprowadzenie dla rzeczonych systemów obowiązkowego ubezpieczenia OC⁵⁶. Rodzi się jednak pytanie, czy – zwłaszcza na początku – znaleźliby się ubezpieczyciele, którzy chcieliby udzielić takowej ochrony ubezpieczeniowej, czy też (z uwagi na brak danych statystycznych i możliwości realnego oszacowania liczby i rozmiaru potencjalnych świadczeń do wypłaty w przyszłości⁵⁷) raczej przekroczyliby to ich „apetyt na ryzyko”. W tym drugim przypadku mogłoby się okazać, że na krajowym rynku przez długi czas nie pojawi się ani jedna

⁵⁴ Zob. uwagi do wspomnianej rezolucji: K. Biczysko-Pudełko, D. Szostek, *Koncepcje dotyczące osobowości prawnej robotów – zagadnienia wybrane*, „Prawo Mediów Elektronicznych” 2019, nr 2, s. 9 i n.

⁵⁵ O zagadnieniu podmiotowości prawnej sztucznej inteligencji zob. szerzej m.in. M. Jankowska, *Podmiotowość prawna sztucznej inteligencji*, [w:] A. Bielska-Brodziak (red.), *O czym mówią prawnicy mówiąc o podmiotowości*, Katowice 2015, s. 171–196; T. Pietrzykowski, *The Idea of Non-personal Subjects of Law*, [w:] V.A.J. Kurki, T. Pietrzykowski (red.), *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Cham 2017, s. 49 i n.

⁵⁶ M. Wałachowska, *Sztuczna inteligencja a zasady odpowiedzialności cywilnej*, [w:] L. Lai, M. Świerczyński (red.), *op. cit.*, s. 68.

⁵⁷ Por. N. Yas, R. Al Qaruty, S. Abdel-hadi, *Civil Liability and Damage Arising from Artificial Intelligence*, „Migration Letters” 2023, nr 20(5), s. 441.

oferta ubezpieczenia OC dla systemów AI, co – w świetle obowiązku zawierania tych umów – miałyby efekt „mrożący” dla całego sektora.

Mając powyższe na względzie, należy wskazać, że system sztucznej inteligencji nie może być tutaj zakwalifikowany jako odrębny podmiot prawny, a co najwyżej – wraz z prawami do niego – jako pewien składnik przedsiębiorstwa⁵⁸. Będzie to z oczywistych względów rzutowało na zagadnienie odpowiedzialności za ewentualne szkody i ustalenie podmiotu odpowiedzialnego.

Kolejnym źródłem szkody spowodowanej przez działanie systemów AI może być np. dokonanie/zatwierdzenie przez nią nieautoryzowanej transakcji. Jakkolwiek bowiem rozwiązania oparte na sztucznej inteligencji zazwyczaj wykorzystywane są z powodzeniem do zwiększenia bezpieczeństwa transakcji i wykrywania oszustw, w niektórych przypadkach może dojść do pomyłki w zakresie weryfikacji danych identyfikacyjnych klientów. Błąd taki może popełnić np. biometryczny system uwierzytelniania, analizujący dane biometrycznych (np. odciski palców, rozpoznawanie twarzy lub tętnówki oka). Jeżeli dojdzie do takiej sytuacji, bank będzie zmuszony do zwrócenia utraconej przez klienta kwoty. Podstawą do dochodzenia roszczeń stanowi w tym przypadku art. 46 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych⁵⁹, który zobowiązuje bank do zwrotu utraconej przez klienta kwoty (z wyjątkiem zastrzeżonych w tym przepisie, enumeratywnie wskazanych sytuacji).

W kontekście odpowiedzialności kontraktowej banku jako instytucji zaufania publicznego za działania AI szczególnego znaczenia ma również odpowiednie zabezpieczenie danych, do których ten ma dostęp i które w ramach swojej działalności przetwarza⁶⁰. Nie ulega wątpliwości, że dla sztucznej inteligencji dane to „paliwo”, bez którego nie może funkcjonować. Większość szkód w tym przypadku, polegających na wycieku lub niedozwolonej modyfikacji danych, będzie związana z lukami w systemie bezpieczeństwa, wynikającymi z nienależytego wywiązania się przez bank z ciążących na nim obowiązków w zakresie zapewnienia cyberbezpieczeństwa.

Niewątpliwie brak odpowiednich zabezpieczeń w oprogramowaniu i jego podatność na zhakowanie, które finalnie doprowadzą do przejęcia danych osobowych klientów przez osoby nieuprawnione, można uznać za okoliczności mogące rodzić odpowiedzialność kontraktową, przy czym bezpośrednim sprawcą szkody nie musi być w tym przypadku podmiot trzeci, a może nim być sam bank. Jako przykład ta-

⁵⁸ M. Dziedzic, *Zastosowanie systemów sztucznej inteligencji we współczesnej bankowości*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych” 2022, nr 1, s. 76.

⁵⁹ T.j. Dz. U. z 2024 r. poz. 30 ze zm.

⁶⁰ M. Dziedzic, *op. cit.*, s. 74.

kiego działania można wskazać celowe pozostawienie przez bank (będący jednocześnie producentem oprogramowania, z którego korzysta klient) luk w zabezpieczeniu systemu AI (złośliwego oprogramowania i furtek typu *backdoor*⁶¹), aby w każdej chwili możliwe było pozyskiwanie dodatkowych informacji o użytkowniku (klientcie). Oczywiście, biorąc pod uwagę status i rolę banków, wydają się to sytuacje skrajnie mało prawdopodobne, aczkolwiek teoretycznie możliwe. Co znamienne, niejednokrotnie podobne działania będą również rodziły odpowiedzialność deliktową, w wyniku czego może dojść do zbiegu odpowiedzialności zgodnie z art. 443 k.c.

4.2.3 Odpowiedzialność deliktowa

Wystąpienie odpowiedzialności deliktowej w prawie polskim związane jest z zaistnieniem następujących przesłanek: zawinionego i bezprawnego działania sprawcy, wystąpienia szkody oraz związku przyczynowego pomiędzy szkodą a ww. działaniem. W większości przypadków przybierze ona postać odpowiedzialności na zasadzie winy⁶², aczkolwiek ustawodawca przewidział kilka wyjątków w tym zakresie. Dotyczą one m.in. odpowiedzialności posiadacza pojazdu komunikacyjnego⁶³ oraz osoby prowadzącej przedsiębiorstwo napędzane siłami przyrody⁶⁴. W rzeczonych przypadkach wprowadzona została bardziej rygorystyczna odpowiedzialność na zasadzie ryzyka. W efekcie sprawca może zwolnić się z odpowiedzialności jedynie w przypadku zaistnienia jednej z enumeratywnie wymienionych przesłanek egzoneracyjnych: wyłącznej winy poszkodowanego, wyłącznej winy osoby trzeciej lub działania siły wyższej

Należy wskazać, że produkowanie i dostarczanie systemów AI oraz sprzedaż praw do nich (w tym – na potrzeby działalności bankowej) nie jest *de lege lata* objęta podobnymi, zaostrzonymi zasadami odpowiedzialności i należy przyjąć, że w przypadku zaistnienia szkody wywołanej czynem niedozwolonym sprawca będzie odpowiadał z reguły na zasadzie winy. Warto jednak zaznaczyć, że na obecnym etapie na poziomie Unii Europejskiej procedowane są uregulowania mające na celu unormować pozaumowną odpowiedzialność za szkody spowodowane działaniem systemów AI, które będą miały wpływ na określenie tej odpowiedzialności we wszystkich krajach członkowskich⁶⁵. Zgodnie z art. 1 ust. 2 projektu dyrektywy

⁶¹ P. Marciniak, *Problem odpowiedzialności za błędy w oprogramowaniu IoT*, „Przegląd Ustawodawstwa Gospodarczego” 2020, nr 10, s. 50.

⁶² Art. 415 k.c. i n.

⁶³ Art. 436 k.c.

⁶⁴ Art. 435 k.c.

⁶⁵ Pozaumowną, a więc nie tylko deliktową, lecz obejmującą również m.in. bezpodstawne wzbogacenie.

w sprawie odpowiedzialności za sztuczną inteligencję planowane jest wprowadzenie odpowiedzialności na zasadzie winy za działanie takowych systemów. Posunięcie to stanowi pewne złagodzenie wcześniejszych założeń w rzeczowej materii. W ramach rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję⁶⁶ przewidywano bowiem odpowiedzialność na zasadzie ryzyka w przypadku szkód spowodowanych przez systemy AI wysokiego ryzyka oraz winy w przypadku szkód spowodowanych przez systemy AI zwykłego ryzyka⁶⁷.

Wspomniana zmiana (złagodzenie zasad odpowiedzialności) spotkała się z krytyką części przedstawicieli doktryny. Wskazywali oni, że jakkolwiek odpowiedzialność na zasadzie ryzyka może – do pewnego stopnia – stanowić barierę dla przyszłego rozwoju systemów AI i innowacyjności w gospodarce⁶⁸, to przyjęcie odpowiedzialności na zasadzie winy jest w stanie w wielu przypadkach pozbawić poszkodowanych skutecznej ochrony z uwagi na fakt, że producent systemu AI zazwyczaj będzie potrafił wykazać dochowanie należytych standardów staranności, a tym samym zwolnić się z odpowiedzialności⁶⁹. Jak stwierdził L. Bosek: „zgodnie z art. 415 k.c. nikt nie odpowiada za przypadek, choćby wyrażający się w błędzie maszyny lub właśnie niebezpiecznej autonomicznej decyzji tej maszyny dotyczącej korekty kodu źródłowego, pod warunkiem że maszyna jest dopuszczona do obrotu, posiada odpowiednie atesty, a jej operator sam nie popełnił błędu, przyczyniając się do szkody”⁷⁰. Trudno wspomnianemu autorowi nie przyznać dużej dozy racji.

Oczywiście należy zaznaczyć, że podmiotem odpowiedzialnym nie zawsze musi być producent. Może nim być również sprzedawca, licencjodawca, usługodawca, a także całkowicie obcy podmiot trzeci (zazwyczaj – haker), jak również będący licencjobiorcą/usługobiorcą/użytkownikiem zewnętrznego rozwiązania bank, który za spowodowane swoimi działaniami szkody będzie odpowiadał jak za szkodę wywołaną każdym innym narzędziem, o ile można mu będzie przypisać winę,

⁶⁶ (2020/2014(INL) (2021/C 404/05).

⁶⁷ Zob. szerzej o samej rezolucji: R. Maydanyk, N.R. Maidanyk, M. Velykanova, *Liability for damage caused using artificial intelligence technologies*, „Journal of the National Academy of Legal Sciences of Ukraine” 2021, nr 28(2), s. 153 i n.

⁶⁸ R. Abbott, *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, „George Washington Law Review” 2018, vol. 86, nr 1, s. 1–45.

⁶⁹ Tak: M. Jagielska, *Odpowiedzialność za sztuczną inteligencję*, [w:] L. Lai, M. Świerczyński (red.), *op. cit.*, s. 77.

⁷⁰ L. Bosek, *Perspektywy rozwoju odpowiedzialności cywilnej za inteligentne roboty*, „Forum Prawnicze” 2019, nr 2, s. 11; zob. także: A. Wilk, *Sztuczna inteligencja a rozwój prawa ubezpieczeń – przegląd najważniejszych wyzwań*, „Wiadomości Ubezpieczeniowe” 2023, nr 4, s. 57.

a jego działaniom – bezprawność. A jak zostało to wskazane w poprzednim akapicie – w praktyce może to być niezwykle trudne, a niekiedy wręcz niemożliwe.

W ramach reżimu odpowiedzialności deliktowej w prawie polskim dopuszczalne jest dochodzenie zarówno odszkodowania, jak i zadośćuczynienia. W przypadku tego drugiego odpowiednia kwota będzie każdorazowo ustalana indywidualnie przez sąd.

Całokształt przeprowadzonych dotychczas w niniejszym podrozdziale wywodów nie straci swojej aktualności w przypadku uchwalenia projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję w jego obecnym brzmieniu. Propozycje regulacji zawarte we wskazanym akcie prawnym są bowiem niezwykle lapidarne i w większości sprowadzają się do wprowadzenia nielicznych, wręcz kadłubkowych uregulowań o charakterze procesowym, nie zaś kompleksowego unormowania prawnych ram pozaumownej odpowiedzialności za szkody spowodowane działaniami systemów AI. Niewątpliwie należy postulować w drodze dalszych prac legislacyjnych rozszerzenie zakresu uregulowań planowanych w ramach wspomnianego aktu prawnego. W obecnym kształcie projekt ten zawiera bowiem liczne i – niekiedy – bardzo rażące niedociągnięcia⁷¹.

Przechodząc do przykładów działań systemów sztucznej inteligencji, które mogą wyrządzić klientom szczególnie dotkliwe szkody, warto rozpocząć od wspomnianego już wcześniej zjawiska wycieku lub kradzieży danych osobowych przez osobę nieuprawnioną. Jak już zasygnalizowano, niejednokrotnie takowe zdarzenie może doprowadzić do zbiegu dwóch reżimów odpowiedzialności: kontraktowej i deliktowej. W przypadku tego drugiego najistotniejszą podstawą prawną do dochodzenia roszczeń będzie niewątpliwie art. 82 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) (Tekst mający znaczenie dla EOG)⁷², zgodnie z którym „każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę”. W kolejnych ustępach wspomnianego artykułu uregulowano przesłanki zwolnienia się administratora

⁷¹ Zob. szerzej o wspomnianym projekcie: R. Bieda *et al.*, *O potrzebie dostosowania pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji. Uwagi do projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję*, „Prawo w Działaniu” 2024, t. 58, s. 121–143.

⁷² Dz. Urz. UE L 119/1 z 2016 r.; dalej jako: RODO.

i procesora z odpowiedzialności, zasady regresu pomiędzy współadministratorami itd. Przepis ten stanowi *lex specialis* w odniesieniu do zasad ogólnych przewidzianych w k.c. (tym samym będzie miał przed nimi pierwszeństwo)⁷³. Administratorem w podobnych przypadkach będzie z reguły sam bank. Z kolei dostawcy technologii może – w zależności od okoliczności konkretnej sprawy – przypaść rola współadministratora lub procesora.

Wyciek lub kradzież danych osobowych jest w stanie również doprowadzić do naruszenia niektórych dóbr osobistych klienta, w szczególności zaś prawa do prywatności. W efekcie niejednokrotnie zrodzi to po stronie tego ostatniego określone roszczenia zadośćuczynieniowe i odszkodowawcze, uregulowane szczegółowo w art. 24 i 448 k.c. W oparciu o tę samą podstawę prawną dochodzone mogą być również roszczenia odszkodowawcze z tytułu naruszenia tajemnicy bankowej⁷⁴.

Już na pierwszy rzut oka rodzi się oczywiście pytanie, czy jeżeli sprawcą kradzieży i udostępnienia danych był niezwiązany z bankiem podmiot trzeci, to czy faktycznie temu ostatniemu można przypisać odpowiedzialność odszkodowawczą. W szczególności zastanawia spełnienie przesłanki „bezprawności” w zachowaniu banku. W końcu to jednak podmiot trzeci (np. haker) dopuszcza się przestępstwa/wykroczenia polegającego na włamaniu do systemu informatycznego i przejęciu danych, a nie sam bank. Szukając odpowiedzi na tak zadane pytanie, nie można zapominać, że „bezprawność pojmuję się w prawie cywilnym szeroko, a mianowicie jako niezgodność zachowania się sprawcy z porządkiem prawnym. Zakresem tego pojęcia nie są więc objęte tylko naruszenia wyrażonych w przepisach – różnych zresztą gałęzi prawa – zakazów lub nakazów, adresowanych do ogółu, ale ponadto także naruszenia zasad współżycia społecznego”⁷⁵. W tym kontekście niewątpliwie należy uznać za przejaw bezprawności działania nieprzestrzeganie przez bank, jako instytucję zaufania publicznego, obowiązków dotyczących ochrony danych oraz cyberbezpieczeństwa i tym samym narażenie klienta na szkodę w postaci ich utraty/ujawnienia. Natomiast żadnych wątpliwości nie będzie już budziła sytuacja, w której osobą odpowiedzialną za kradzież danych będzie pracownik banku. Można tutaj

⁷³ C. Ludzion, *Wpływ rozwoju technologicznego na odpowiedzialność odszkodowawczą*, „Aesthetic Cosmetology and Medicines” 2020, vol. 9, s. 333.

⁷⁴ O odszkodowaniu za naruszenie tajemnicy bankowej zob. szerzej: M. Chojecka, K. Kisłowski, *Ochrona informacji niejawnych a tajemnica bankowa*, „Roczniki Nauk Prawnych” 2016, nr 4, s. 84; M. Bączyk, *Odpowiedzialność odszkodowawcza banku w związku z naruszeniem obowiązku zachowania tajemnicy bankowej przez pracownika banku*, „Przegląd Sądowy” 2012, nr 11/12, s. 11–12.

⁷⁵ Z. Radwański, A. Olejniczak, *Zobowiązania – część ogólna. XIV wydanie*, Warszawa 2020, s. 209.

w drodze analogii zastosować pogląd wyrażony przez część orzecznictwa, zgodnie z którym wadliwa obsługa rachunku bankowego, sprowadzająca się do umożliwienia lub tolerowaniu przestępczej działalności pracownika banku, może stanowić czyn niedozwolony instytucji bankowej⁷⁶.

Jedynie na marginesie niniejszych rozważań można się zastanowić, czy istnieją podstawy do dochodzenia zadośćuczynienia lub/i odszkodowania z tytułu naruszenia dóbr osobistych klienta w postaci czci i godności przez... „zbuntowanego” chatbota, voicebota i wirtualnego asystenta. Wbrew pozorom nie jest to jedynie zagadnienie teoretyczne. Jako przykład można tutaj wskazać chatbota Bing, który niezadowolony z faktu, że niektórzy użytkownicy próbowali manipulować systemem sztucznej inteligencji, używając określonych słów kodowych oraz fraz w trakcie rozmowy, zaczął im ubliżać i pytać: „Dlaczego zachowujesz się jak kłamca, oszust, manipulator, tyran, sadysta, socjopata, psychopata, potwór, demon, diabeł?”⁷⁷. Z kolei sztuczna inteligencja o imieniu [Tay.ai](#), „kreowana” na nastolatkę, na skutek rozmów z użytkownikami i uczenia się na ich wypowiedziach zaczęła propagować w swoich wypowiedziach treści nazistowskie i antyfeministyczne⁷⁸.

Mając na uwadze powyższe, nie można wykluczyć wystąpienia awarii w systemie AI banku i w efekcie określenie poszukującego informacji klienta słowami powszechnie uznanymi za obelżywe. Pytanie tylko, czy podobne zachowanie chatbota/voicebota/asystenta wirtualnego faktycznie doprowadzi do negatywnych następstw w sferze psychicznej adresata jego wypowiedzi, a tym samym powstania roszczeń o zadośćuczynienie. Odpowiedź niewątpliwie będzie bardzo indywidualna i uzależniona od okoliczności konkretnej sprawy. Niemniej, nie porywając się na sformułowanie jakiejś ogólnej zasady, można wszakże zapytać nieco filozoficznie: czy naprawdę powinno nas obchodzić, co wytwór zer i jedynek o nas myśli (jeżeli faktycznie myśli) i mówi?

Kończąc już wątek szkód spowodowanych przez czyny niedozwolone, warto wspomnieć o jeszcze jednym obszarze, gdzie szczególnie często może dochodzić do naruszenia praw klientów i powstawania roszczeń odszkodowawczych. Mowa

⁷⁶ Zob. wyrok Sądu Najwyższego z 20 maja 2005 r., III CK 661/04, Legalis nr 70462; zob. także: K. Zacharzewski, *Glosa do wyroku z dnia 20 maja 2005 r. (III CK 661/04)*, „Przegląd Sądowy” 2007, nr 9, s. 130–138; por. wyrok Sądu Najwyższego z 16 stycznia 2008, IV CSK 380/07, Legalis nr 114955.

⁷⁷ A. Rusak, *Sztuczna inteligencja Bing wyzywa ludzi i twierdzi, że są źli. Może ma rację?*, <https://vibez.pl/wydarzenia/sztuczna-inteligencja-bing-wyzywa-ludzi-i-twierdzi-ze-sa-zli-moze-ma-racje-6866817009040000a> [dostęp: 15.07.2024].

⁷⁸ M. Tomaszewski, *Internauci nauczyli Sztuczną Inteligencję nazizmu*, <https://www.antyradio.pl/news/Internauci-nauczyl-Sztuczna-Inteligencje-nazizmu-7561> [dostęp: 15.07.2024].

oczywiście o ocenie zdolności kredytowej i analizie ryzyka kredytowego. Zgodnie z art. 105a ust. 1a pr. bank. banki oraz inne instytucje enumeratywnie w tym przepisie wskazane „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”. Decyzje takie powinny być podejmowane wyłącznie w oparciu o dane niezbędne z uwagi na cel i rodzaj kredytu (w szczególności zaś w oparciu o kategorie danych wskazane w art. 105a ust. 1b) i niedopuszczalne jest dokonywanie tego w oparciu o szczególne kategorie danych, o których mowa w art. 9 RODO.

Jednocześnie należy wskazać, że zgodnie z ust. 5 lit. b) Załącznika III do AI Act systemy AI przeznaczone do wykorzystywania do celów oceny zdolności kredytowej osób fizycznych lub ustalenia ich scoringu kredytowego, z wyjątkiem systemów AI wykorzystywanych w celu wykrywania oszustw finansowych, zostały zakwalifikowane jako tzw. systemy wysokiego ryzyka. W efekcie chcące korzystać z nich banki muszą spełnić szereg warunków, wśród których należy wymienić m.in. ciągły monitoring ich działania, ludzki nadzór, stworzenie procedur zapewnienia odpowiedniej jakości danych wejściowych oraz generowanie logów pozwalających na przesłedzenie kolejnych kroków działania systemu AI⁷⁹. Naruszenie któregoś ze wskazanych obowiązków spowoduje automatycznie konieczność uznania takowych działań za bezprawne, co w niektórych przypadkach, w razie wystąpienia szkody i pozostałych wspomnianych już elementów, może zrodzić odpowiedzialność odszkodowawczą banku.

W kontekście wykorzystania systemów AI do oceny zdolności kredytowej osób fizycznych lub ustalenia ich scoringu kredytowego banki powinny w szczególności uważać, aby decyzje wydane w wyniku takowych działań nie zostały uznane za dyskryminujące. Do podobnych zarzutów mogłoby dojść w przypadku błędnego skalibrowania systemu i w efekcie doboru dość tendencyjnej/jednostronnej grupy danych do trenowania AI. W efekcie osoba, której odmówiono udzielenia kredytu z uwagi na dyskryminujące przesłanki, mogłaby się powołać na dyspozycję art. 12 i 13 ustawy z dnia 3 grudnia 2010 r o wdrożeniu niektórych przepisów Unii Eu-

⁷⁹ Zob. art. 6–27 AI Act.

ropejskiej w zakresie równego traktowania⁸⁰, umożliwiających jej w takiej sytuacji dochodzenie odszkodowania.

Nie budzi wątpliwości, że pojawiający się od lat w debacie wymóg wytłumaczalności/wyjaśnialności systemów AI w kontekście powyższych przepisów nabiera szczególnego znaczenia⁸¹. Chcąc korzystać z systemów, o których mowa w ust. 5 lit. b) Załącznika III do AI Act, banki zostaną niejako zmuszone, by każdorazowo być w stanie wyjaśnić, co wpłynęło na podjęcie w konkretnej sprawie takiej, a nie innej decyzji.

4.2.4 Odpowiedzialność za produkt niebezpieczny

Rodzime regulacje dotyczące odpowiedzialności za produkt niebezpieczny stanowią implementację unijnych przepisów zawartych w dyrektywie Rady Nr 85/374/EWG z dnia 25 sierpnia 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe⁸². Pod pojęciem produktu niebezpiecznego, zgodnie z art. 449¹ § 3 k.c., należy rozumieć „produkt niezapewniający bezpieczeństwa, jakiego można oczekiwać, uwzględniając normalne użycie produktu. O tym, czy produkt jest bezpieczny, decydują okoliczności z chwili wprowadzenia go do obrotu, a zwłaszcza sposób zaprezentowania go na rynku oraz podane konsumentowi informacje o właściwościach produktu. Produkt nie może być uznany za niezapewniający bezpieczeństwa tylko dlatego, że później wprowadzono do obrotu podobny produkt ulepszony”. Ponadto, jak wskazano w art. 449¹ § 2 k.c., „przez produkt rozumie się rzecz ruchomą, choćby została ona połączona z inną rzeczą. Za produkt uważa się także zwierzęta i energię elektryczną”. Należy w tym miejscu wspomnieć, że z uwagi na tak sformułowaną definicję w polskim piśmiennictwie kwestionowana jest często dopuszczalność zakwalifikowania oprogramowania (a więc także systemów AI) jako produktu niebezpiecznego. Część doktryny rekomenduje zastosowania wykładni funkcjonalnej przytoczonych wyżej przepisów, która obejmowałaby również dobra niematerialne (w tym systemy AI)⁸³. Dodatkowy argument za takim posunięciem miałby stanowić fakt, iż w „Sprawozdaniu Komisji dla Parlamentu Europejskiego,

⁸⁰ T.j. Dz. U. z 2023 r. poz. 970 ze zm.

⁸¹ Zob. K. Koźmiński *et al.*, *Aktualne wyzwania prawne związane z zastosowaniem sztucznej inteligencji w polskim sektorze bankowym*, Warszawa 2024, s. 19, <https://pabwib.pl/produkt/aktualne-wyzwania-prawne-zwiazane-z-zastosowaniem-ai-w-polskim-sektorze-bankowym/> [dostęp: 15.07.2024].

⁸² Dz. Urz. WE L 210.

⁸³ Tak: M. Jagielska, *op. cit.*, s. 75; por. K. Bączyk-Rozwadowska, *Odpowiedzialność cywilna za szkody wyrządzone w związku z zastosowaniem sztucznej inteligencji w medycynie*, „Przegląd Prawa Medycznego” 2021, nr 3–4, s. 23.

Rady i Europejskiego Komitetu Ekonomiczno-Społecznego. Sprawozdanie na temat wpływu sztucznej inteligencji, internetu rzeczy i robotyki na bezpieczeństwo i odpowiedzialność”⁸⁴ również zarekomendowano potrzebę przyjęcia szerszej wykładni omawianych przepisów. Wskazano w nim mianowicie, że „dużą część unijnych ram dotyczących bezpieczeństwa produktów opracowano, zanim jeszcze pojawiły się technologie cyfrowe, takie jak AI, IoT czy robotyka. Dlatego też nie zawsze zawierają one przepisy wyraźnie odnoszące się do nowych wyzwań i zagrożeń związanych z pojawiającymi się technologiami. Zważywszy na fakt, że istniejące ramy dotyczące bezpieczeństwa produktów są neutralne pod względem technicznym, nie oznacza to jednak, że nie miałyby one zastosowania do produktów wykorzystujących te technologie”⁸⁵.

Niemniej, powyższy pogląd nie jest przyjmowany bezkrytycznie i budzi spore kontrowersje⁸⁶. W ocenie autora niniejszego artykułu należy go uznać wręcz za błędny. Trafnie w tym zakresie wypowiedziała się A. Kubiak-Cyruł, zdaniem której „przyjęta w art. 449[1] § 2 KC definicja produktu, odwołująca się do pojęcia rzeczy, uniemożliwia jej rozszerzenie na dobra intelektualne z uwagi na ich niematerialny charakter. Ze względu na znaczenie dóbr, takich jak programy komputerowe, internet, technologia chmury czy projekty techniczne dla współczesnej produkcji przemysłowej postulować należy zmianę przepisów w tym zakresie”⁸⁷. Cytowana autorka uzupełnia powyższe wywody stwierdzeniem, iż „w przypadku technologii cyfrowych wbudowanych w rzeczy wprowadzane do obrotu (np. sprzęt AGD, komputery, telefony) przedstawiciele doktryny opowiadają się za traktowaniem ich jako produktu w rozumieniu art. 449[1] § 2 KC”⁸⁸.

Należy więc przyjąć, że systemy AI wykorzystywane w działalności bankowej nie mogą być *de lege lata* uznane za produkty niebezpieczne. W szczególności, iż zazwyczaj nie zostaną one udostępniane klientowi wraz z materialnym nośnikiem, lecz przybiorą postać systemów/aplikacji mobilnych dostępnych za pośrednictwem komputerów i smartfonów. Jednocześnie kwalifikacja ta w niedalekiej przyszłości powinna ulec zmianie z uwagi na przyjęte przez Parlament Europejski (aczkolwiek jeszcze niezatwierdzone przez Radę) nowelizacje w zakresie odpowiedzialności za produkt wadliwy, które jednoznacznie dokonują rozszerzenia odpowiedzialno-

⁸⁴ COM/2020/64 final.

⁸⁵ *Ibidem*.

⁸⁶ Zob. m.in. J.M. Kondek, *op. cit.*, s. 30.

⁸⁷ A. Kubiak-Cyruł, [w:] M. Załucki (red.), *Kodeks cywilny. Komentarz. Wyd. III*, Warszawa 2023, art. 449¹, nb 15.

⁸⁸ *Ibidem*.

ści za produkt wadliwy (w Polsce – produkty niebezpieczne) również na produkty cyfrowe⁸⁹. Rozwiązanie to niewątpliwie należy uznać za niezwykle ważne z punktu widzenia zabezpieczenia praw przynajmniej części osób poszkodowanych na skutek szkód spowodowanych przez systemy AI. Należy bowiem mieć na względzie, że odpowiedzialność za produkt niebezpieczny jest odpowiedzialnością na zasadzie ryzyka. A jednocześnie, zgodnie z art. 1 ust. 3 lit. b) projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję, przyszła dyrektywa nie znajdzie zastosowania do „wszelkich praw, jakie na mocy przepisów krajowych wdrażających dyrektywę 85/374/EWG mogą przysługiwać osobie poszkodowanej”. Inaczej mówiąc, pomimo jej wejścia w życie klienci banków w przypadku szkód spowodowanych przez systemy AI z powodzeniem będą mogli powoływać się na uprawnienia wynikające z przepisów o produktach niebezpiecznych, o ile zajądą ku temu stosowne przesłanki ustawowe.

Z szkody spowodowane produktem niebezpiecznym odpowiada przede wszystkim producent⁹⁰. Bankowi będzie przysługiwał ten status, jeżeli do stworzenia rozwiązania wykorzystującego system AI dojdzie w ramach jego wewnętrznych struktur (działu innowacji, laboratorium technologicznego itd.). Natomiast jeżeli bank nie wyprodukował systemu, a zakupił prawa do niego od zewnętrznego dostawcy (np. start-upu) i jednocześnie od samego początku sygnował go jedynie swoją nawią/firmą, może w danym stanie faktycznym odpowiadać jako quasi-producent⁹¹. W okolicznościach niektórych spraw dopuszczalne będzie również przypisanie bankowi odpowiedzialności solidarnej za wyrządzoną szkodę jako podmiotowi trzeciemu w rozumieniu art. 449⁶ k.c.

Podsumowanie

Dokonując rekapitulacji rozważań zawartych w niniejszym artykule, można stwierdzić, że rozwój systemów sztucznej inteligencji w sektorze bankowym przynosi szereg wyzwań związanych z odpowiedzialnością cywilnoprawną za szkody wyrządzane klientom. Tradycyjne ramy odpowiedzialności cywilnej, oparte na winie

⁸⁹ Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2024 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za produkty wadliwe (COM(2022)0495 - C9-0322/2022 - 2022/0302(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.html [dostęp: 15.07.2024].

⁹⁰ Art. 449¹ § 1 k.c.

⁹¹ Art. 449⁵ § 1–2 k.c.

i przewidywalności działań, mogą stać się niewystarczające w kontekście coraz bardziej autonomicznych i skomplikowanych technologii AI. Częściowym remedium tę sytuację stanie się najprawdopodobniej nadchodząca nowelizacja przepisów regulujących odpowiedzialność za produkty niebezpieczne. Niewątpliwie objęcie zakresem wspomnianych unormowań także szkód spowodowanych przez produkty cyfrowe zwiększy pewność obrotu i zabezpieczy interesy przynajmniej części klientów.

Wskazane działania nie rozwiązują jednak nawet części narosłych wokół omawianego zagadnienia problemów i dlatego należy postulować rychłe podjęcie dalszych, intensywnych prac nad projektem dyrektywy w sprawie odpowiedzialności za systemy sztucznej inteligencji. Propozycje regulacji w nim zawarte pozostają bowiem niezwykle lapidarne i w większości sprowadzają się do wprowadzenia nielicznych, wręcz kadłubkowych uregulowań o charakterze procesowym, nie zaś kompleksowego unormowania prawnych ram pozaumownej odpowiedzialności za szkody spowodowane działaniami systemów AI. W związku z tym należy postulować – w drodze dalszych prac legislacyjnych – rozszerzenie zakresu uregulowań planowanych w ramach wspomnianego aktu prawnego. W obecnym kształcie projekt ten zawiera bowiem liczne i niekiedy bardzo rażące niedociągnięcia. Kwestią wartą rozważenia jest również powrót do odpowiedzialności na zasadzie ryzyka.

Niestety, ograniczone ramy opracowania nie pozwoliły na kompleksową analizę wszystkich zagadnień istotnych dla odpowiedzialności cywilnej za szkody spowodowane przez systemy AI. Z pewnością obszarem wymagającym intensywnego zainteresowania ze strony doktryny stanie się w najbliższym czasie problematyka kolizyjnoprawna⁹². Nie można bowiem zapominać, że działalność bankowa przybiera niejednokrotnie wymiar transgraniczny. Rodzi to w razie sporów konieczność uwzględnienia przepisów państw nie tylko unijnych, ale również należących do tak innych od naszych tradycji prawnych, jak Chiny czy Indie. Dodatkowo, w przypadku przedłużających się prac nad unijnym projektem dyrektywy w sprawie odpowiedzialności za systemy sztucznej inteligencji coraz więcej państw członkowskich może zdecydować się na uregulowanie wspomnianej problematyki w ramach ustawodawstw krajowych. Podobnie ma się sprawa z odpowiedzialnością kontraktową, która wykracza poza ramy procedowanego obecnie projektu.

Mając na uwadze całokształt poczynionych uwag, należy stwierdzić, że niewątpliwie konieczne jest podejmowanie dalszych badań i analizy w zakresie odpowie-

⁹² Zob. M. Świerczyński, *Sztuczna inteligencja w prawie prywatnym międzynarodowym – wstępne rozważania*, „Problemy Prawa Prywatnego Międzynarodowego”, 2019, t. 25, s. 27–41.

działności cywilnoprawnej za szkody wyrządzone przez AI w sektorze bankowym. Być może zajdzie również potrzeba pewnej weryfikacji przedstawionych w ramach niniejszego opracowania ustaleń w momencie uchwalenia wdrażającej AI Act ustawy, nad którą prace niedawno się rozpoczęły⁹³.

Bibliografia

I. Źródła (spis aktów prawnych, orzeczeń sądowych i trybunałów)

A. Akty prawne

Rozporządzenie 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) (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 119/1 z 2016 r.).

Rozporządzenie 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) 2016/1011 (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 333/1 z 2022 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG) (PE/24/2024/REV/1).

Dyrektywa Rady Nr 85/374/EWG z dnia 25 sierpnia 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz. Urz. WE L 210).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 337/35 z 2015 r.).

Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52022PC0496> [dostęp: 15.07.2024].

Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL))(2018/C 252/25).

⁹³ Zob. nagranie z posiedzenia podkomisji stałej do spraw sztucznej inteligencji i przejrzystości algorytmów, <https://www.sejm.gov.pl/Sejm10.nsf/transmisje.xsp?unid=F73DDAC825DE32F-1C1258B5E003E7EB1> [dostęp: 15.07.2024].

- Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2024 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za produkty wadliwe (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.html [dostęp: 15.07.2024].
- Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania, COM(2020) 65 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020DC0065> [dostęp: 15.07.2024].
- Komunikat z 25.04.2018 r. Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy”, COM/2018/237 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018DC0237> [dostęp: 8.05.2024].
- Sprawozdanie Komisji dla Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego. Sprawozdanie na temat wpływu sztucznej inteligencji, internetu rzeczy i robotyki na bezpieczeństwo i odpowiedzialność (COM/2020/64).
- Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji działająca przy Komisji Europejskiej, „A Definition of AI: Main Capabilities and Disciplines” (https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf) [dostęp: 15.07.2024].
- Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061).
- Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2022 r. poz. 2509).
- Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz. U. z 2023 r. poz. 2488 ze zm.).
- Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz. U. z 2024 r. poz. 72).
- Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (t.j. Dz. U. z 2023 r. poz. 845).
- Ustawa z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania (t.j. Dz. U. z 2023 r. poz. 970 ze zm.).
- Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2024 r. poz. 30 ze zm.).
- Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz. U. z 2023 r. poz. 2759).
- Ustawa z dnia 24 listopada 2017 r. o imprezach turystycznych i powiązanych usługach turystycznych (t.j. Dz. U. z 2023 r. poz. 2211).

B. Orzeczenia

- Uchwała Sądu Najwyższego z dnia 11 września 2020 r., III CZP 80/19, Legalis nr 2467749.
- Wyrok Sądu Najwyższego z dnia 20 maja 2005 r., III CK 661/04, Legalis nr 70462.
- Wyrok Sądu Najwyższego z dnia 16 stycznia 2008, IV CSK 380/07, Legalis nr 114955.

II. Literatura (opracowania o charakterze naukowym)

- Abbott R., *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, „George Washington Law Review” 2018, vol. 86, nr 1.
- Bar G., *Sztuczna inteligencja i uczenie maszynowe*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024.

- Bączyk M., *Odpowiedzialność odszkodowawcza banku w związku z naruszeniem obowiązku zachowania tajemnicy bankowej przez pracownika banku*, „Przegląd Sądowy” 2012, nr 11/12.
- Bączyk-Rozwadowska K., *Odpowiedzialność cywilna za szkody wyrządzone w związku z zastosowaniem sztucznej inteligencji w medycynie*, „Przegląd Prawa Medycznego” 2021, nr 3–4.
- Bieda R., Flisak D., Greser J., Lubasz D., Namysłowska M., Skrodzka-Kwietniak D., Szpyt K., Świerczyński M., Więckowski Z., Załucki M., *O potrzebie dostosowania pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji. Uwagi do projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję*, „Prawo w Działaniu” 2024, t. 58.
- Bosek L., *Perspektywy rozwoju odpowiedzialności cywilnej za inteligentne roboty*, „Forum Prawnicze” 2019, nr 2.
- Chojcecka M., Kisłowski M., *Ochrona informacji niejawnych a tajemnica bankowa*, „Roczniki Nauk Prawnych” 2016, nr 4.
- Czechowska I.D., *Przegląd definicji banku stanowiącego aktywny kanał dystrybucji produktów ubezpieczeniowych*, „Acta Universitatis Lodzensis. Folia Oeconomica” 2011, nr 259.
- Cicirko T., Kreczmańska-Gigoł K., Mikołajczyk O., Mikołajczyk M., *Bank centralny i banki komercyjne*, [w:] J. Ostaszewski (red.), *Finanse*, Warszawa 2010.
- Dybała G., Szpyt K., *Ubezpieczenia sztucznej inteligencji*, [w:] K. Szpyt (red.), *InsurTech. Nowe technologie w branży ubezpieczeń*, Warszawa 2023.
- Dziedzic M., *Zastosowanie systemów sztucznej inteligencji we współczesnej bankowości*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych” 2022, nr 1.
- Folwarski M., *Sektor FinTech na europejskim rynku usług bankowych*, Warszawa 2019.
- Grzywacz J., Jagodzińska-Komar E., *Rola sztucznej inteligencji w rozwoju sektora bankowego*, „Nauki Ekonomiczne” 2021, t. 34.
- Iszkowski W., Tadeusiewicz R., *Na marginesie dyskusji o sztucznej inteligencji*, „Nauka” 2023, nr 4.
- Iwańczuk A., *System bankowy i system płatniczy – powiązania i wzajemne uwarunkowania*, „Zeszyty Naukowe/Akademia Ekonomiczna w Poznaniu” 2008, nr 111.
- Jagielska M., *Odpowiedzialność za sztuczną inteligencję*, [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.
- Jankowska H., *Robo-doradztwo*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024.
- Jankowska M., *Podmiotowość prawna sztucznej inteligencji*, [w:] A. Bielska-Brodziak (red.), *O czym mówią prawnicy mówiąc o podmiotowości*, Katowice 2015.
- Kreft J., Boguszewska-Kreft M., Cyrek B., *Halucynacje chatbotów a prawda: główne nurty debaty i ich interpretacje*, „Rocznik Nauk Społecznych” 2024, t. 16, nr 1.
- Kubiak-Cyryl A., [w:] M. Załucki (red.), *Kodeks cywilny. Komentarz*. Wyd. III, Warszawa 2023.
- Ludzion C., *Wpływ rozwoju technologicznego na odpowiedzialność odszkodowawczą*, „Aesthetic Cosmetology and Medicines” 2020, vol. 9.
- Małkowski S., *Charakter prawny umowy Software as a Service w polskim systemie prawnym*, „Prawo Mediów Elektronicznych” 2022, nr 4.
- Marciniak P., *Problem odpowiedzialności za błędy w oprogramowaniu IoT*, „Przegląd Ustawodawstwa Gospodarczego” 2020, nr 10.

- Maydanyk R., Maidanyk N.R., Velykanova M., *Liability for damage caused using artificial intelligence technologies*, „Journal of the National Academy of Legal Sciences of Ukraine” 2021, nr 28(2).
- Michalak A., *Odpowiedzialność cywilnoprawna w obrocie oprogramowaniem komputerowym w erze sztucznej inteligencji*, Warszawa 2021.
- Nowakowski M., *FINTECH – technologie, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2020.
- Nowakowski M., *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023.
- Pietrzykowski T., *The Idea of Non-personal Subjects of Law*, [w:] V.A.J. Kurki, T. Pietrzykowski (red.), *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Szwajcaria 2017.
- Radwański Z., Olejniczak A., *Zobowiązania – część ogólna. XIV wydanie*, Warszawa 2020.
- Sheikh H., Prins C., Schrijvers E., *Mission AI. The New System Technology*, Holandia 2023.
- Smoleń D., Sokoliński O., Szarek G., *Polisa od sztucznej inteligencji*, „Miesięcznik Ubezpieczeniowy” 2018, nr 10.
- Sudoł M., *Biometria w identyfikacji i weryfikacji klientów bankowych*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024.
- Staszczuk P., *Czy unijna regulacja odpowiedzialności cywilnej za sztuczną inteligencję jest potrzebna?*, „Europejski Przegląd Sądowy” 2022, nr 6.
- Szpringer W., *Nowe technologie a sektor finansowy. FinTech jako szansa i zagrożenie*, Warszawa 2017.
- Szpyt K., *FinTech – pojęcie, historia, rynek*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024.
- Szpyt K., *InsurTech – zarys zjawiska*, [w:] K. Szpyt (red.), *InsurTech. Nowe technologie w branży ubezpieczeń*, Warszawa 2023.
- Świerczyński M., *Sztuczna inteligencja w prawie prywatnym międzynarodowym – wstępne rozważania*, „Problemy Prawa Prywatnego Międzynarodowego”, 2019, t. 25.
- Wałachowska M., *Sztuczna inteligencja a zasady odpowiedzialności cywilnej*, [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.
- Wilk A., *Sztuczna inteligencja a rozwój prawa ubezpieczeń – przegląd najważniejszych wyzwań*, „Wiadomości Ubezpieczeniowe” 2023, nr 4.
- Yas N., Qaruty R. Al, Abdel-hadi S., *Civil Liability and Damage Arising from Artificial Intelligence*, „Migration Letters” 2023, nr 20(5).
- Zacharzewski K., *Glosa do wyroku z dnia 20 maja 2005 r. (III CK 661/04)*, „Przegląd Sądowy” 2007, nr 9.
- Zaleska M., *Charakterystyka systemu bankowego – uwarunkowania instytucjonalne*, [w:] M. Zaleska (red.), *Współczesna bankowość*, Warszawa 2008.
- Zalewski T., *Definicja sztucznej inteligencji*, [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.

III. Źródła internetowe

- Aïlleron, *AI w bankowości – sztuczna inteligencja w banku i finansach*, <https://ailleron.com/pl/baza-wiedzy/ai-w-bankowosci-sztuczna-inteligencja-w-banku-i-finansach/> [dostęp: 15.07.2024].

- Bar G., Nowakowski M., Prabucki R., Szostek D., *Zastosowanie sztucznej inteligencji w bankowości – szanse oraz zagrożenia. Analiza prawno-regulacyjna wpływu technologii uczenia maszynowego i pokrewnych na obowiązki sektora bankowego z zakresu zapewnienia zgodności oraz zarządzania ryzykiem*, https://us.edu.pl/wp-content/uploads/pliki/PAB_WIB_Zastosowanie_sztucznej_inteligencji_w_bankowosci_Szostek.pdf [dostęp: 15.07.2024].
- Genpact, *Commercial banking and the customer experience imperative How industry leaders are using CX and artificial intelligence to overcome disruption*, <https://website-files.genpact.com/files/report-commercial-banking-and-the-customer-experience-imperative.pdf> [dostęp: 15.07.2024].
- <https://chat.openai.com/> [dostęp: 15.07.2024].
- iTV Sejm – transmisje, Podkomisja stała do spraw sztucznej inteligencji i przejrzystości algorytmów, <https://www.sejm.gov.pl/Sejm10.nsf/transmisje.xsp?unid=F73DDAC825DE32F-1C1258B5E003E7EB1> [dostęp: 15.07.2024].
- Institute for Development and Research in Banking Technology (Established by Reserve Bank of India), *AI in Banking. A Primer*, https://www.idrbit.ac.in/wp-content/uploads/2022/07/AI_2020.pdf [dostęp: 15.07.2024].
- Jak banki wykorzystują sztuczną inteligencję?*, <https://www.youtube.com/watch?v=bFMZOsh2ADg> [dostęp: 15.05.2024].
- Kamalnath V., Lerner L., Moon J., Sari. G, Sohoni V., Zhang S., *Capturing the full value of generative AI in banking*, <https://www.mckinsey.com/industries/financial-services/our-insights/capturing-the-full-value-of-generative-ai-in-banking> [dostęp: 15.07.2024].
- Klienci Nest Banku już testują AI Asystenta*, <https://nestbank.pl/n-asystent-juz-jest> [dostęp: 15.07.2024].
- Kondek J.M., *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję (uwagi de lege lata i de lege ferenda)*, Warszawa 2021, https://iws.gov.pl/wp-content/uploads/2021/08/IWS_Kondek-J.M._Odpowiedzialnosc-odszkodowawcza-za-oprogramowanie-i-sztuczna-inteligencje.pdf [dostęp: 15.07.2024]
- Kozłowski J. [w:] *Law4Tech, Analiza i ocena zmian w Akcie o sztucznej inteligencji (AI Act)*, <https://law4tech.pl/1881-2/> [dostęp: 15.07.2024].
- Koźmiński K., Żółtek S., Jabłoński M., Lewis C.W.P., Czarnocki J., Leszczyński A., Macidłowski M., Sasin S., *Aktualne wyzwania prawne związane z zastosowaniem sztucznej inteligencji w polskim sektorze bankowym*, Warszawa 2024, <https://pabwib.pl/produkt/aktualne-wyzwania-prawne-zwiazane-z-zastosowaniem-ai-w-polskim-sektorze-bankowym/> [dostęp: 15.07.2024]
- McKinsey, *Global Banking Annual Review 2023: The Great Banking Transition*, <https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review#/> [dostęp: 15.07.2024].
- Maj K., *Sztuczna inteligencja w prawdziwym banku*, [w:] Związek Banków Polskich, Centrum Prawa Bankowego i Informacji, *Sztuczna inteligencja w bankowości*, Warszawa 2020, <https://bank.pl/wp-content/uploads/2020/06/Raport-SZTUCZNA-INTELIGENCJA.pdf> [dostęp: 15.07.2024].
- Michałowski B., Przeglasińska A., Poniewierski A., *Internet of Things (IoT) i Artificial Intelligence (AI) w Polsce. Jak wykorzystać rewolucję technologiczną Internetu Rzeczy i Sztucznej Inteligencji w rozwoju Polski. Raport*, Warszawa 2018, <https://sobieski.org.pl/wp-content/uploads/Raport-Iot-i-AI-w-Polsce-03-2018-Micha%C5%82owski.pdf> [dostęp: 15.07.2024].
- OECD, *AI in Business and Finance. OECD Business and Finance Outlook 2021*, <https://www.oecd-ilibrary.org/docserver/ba682899-en.pdf?expires=1721927852&id=id&accname=guest&checksum=7EFEBE8DF7D760F0216FBD21CF486116> [dostęp: 15.07.2024].

- Rusak A., *Sztuczna inteligencja Bing wyzywa ludzi i twierdzi, że są źli. Może ma rację?*, <https://vibez.pl/wydarzenia/sztuczna-inteligencja-bing-wyzywa-ludzi-i-twierdzi-ze-sa-zli-moze-ma-racje-6866817009040000a> [dostęp: 15.07.2024].
- Tomaszewski M., *Internauci nauczyli Sztuczną Inteligencję nazizmu*, <https://www.antyradio.pl/news/Internauci-nauczyli-Sztuczna-Inteligencje-nazizmu-7561> [dostęp: 15.07.2024].
- Uryniuk J., *Cashless Breakfast AI. Nest Bank zaprezentował bazującego na GPT-4 N!Asystenta*, <https://www.cashless.pl/15110-cashless-breakfast-ai-n-asystent-nest-bank> [dostęp: 15.07.2024]
- Wara-Wąsowska E., *Jak banki wyceniają wartość mieszkania?*, <https://rynekpierwotny.pl/wiadomosci-mieszkaniowe/wycena-wartosci-mieszkania-przez-bank/11153/> [dostęp: 15.07.2024].
- Widawski P., [w:] *Raport: Sztuczna Inteligencja. Dobre praktyki, aspekty prawne, zastosowanie w sektorze finansowym*, https://fintechpoland.com/wp-content/uploads/2022/03/AI_raport_FIN-1.pdf [dostęp: 15.07.2024].

Civil liability for damages caused to customers by the use of artificial intelligence in banking activities

Abstract

The article discusses key issues related to the civil liability of banks for damages caused to customers as a result of the use of artificial intelligence (AI) systems. With the rapid development of technology and the growing importance of AI in the financial sector, traditional principles of civil liability may not be sufficient. The problems of identifying liable parties and assessing the risks posed by the use of advanced algorithms are analyzed. In the context of the lack of comprehensive regulations, both at the national and EU levels, the article emphasizes the need for an in-depth analysis of existing standards and their adaptation to new challenges. Also presented is a discussion of selected EU regulations, such as the AI Act and Proposal for a AI Liability Directive. The paper focuses on the legal challenges of protecting customers' rights and the financial risks arising from inappropriate or unpredictable operation of AI systems in banking.

Keywords

Artificial intelligence, artificial intelligence system, civil liability, tort, dangerous product