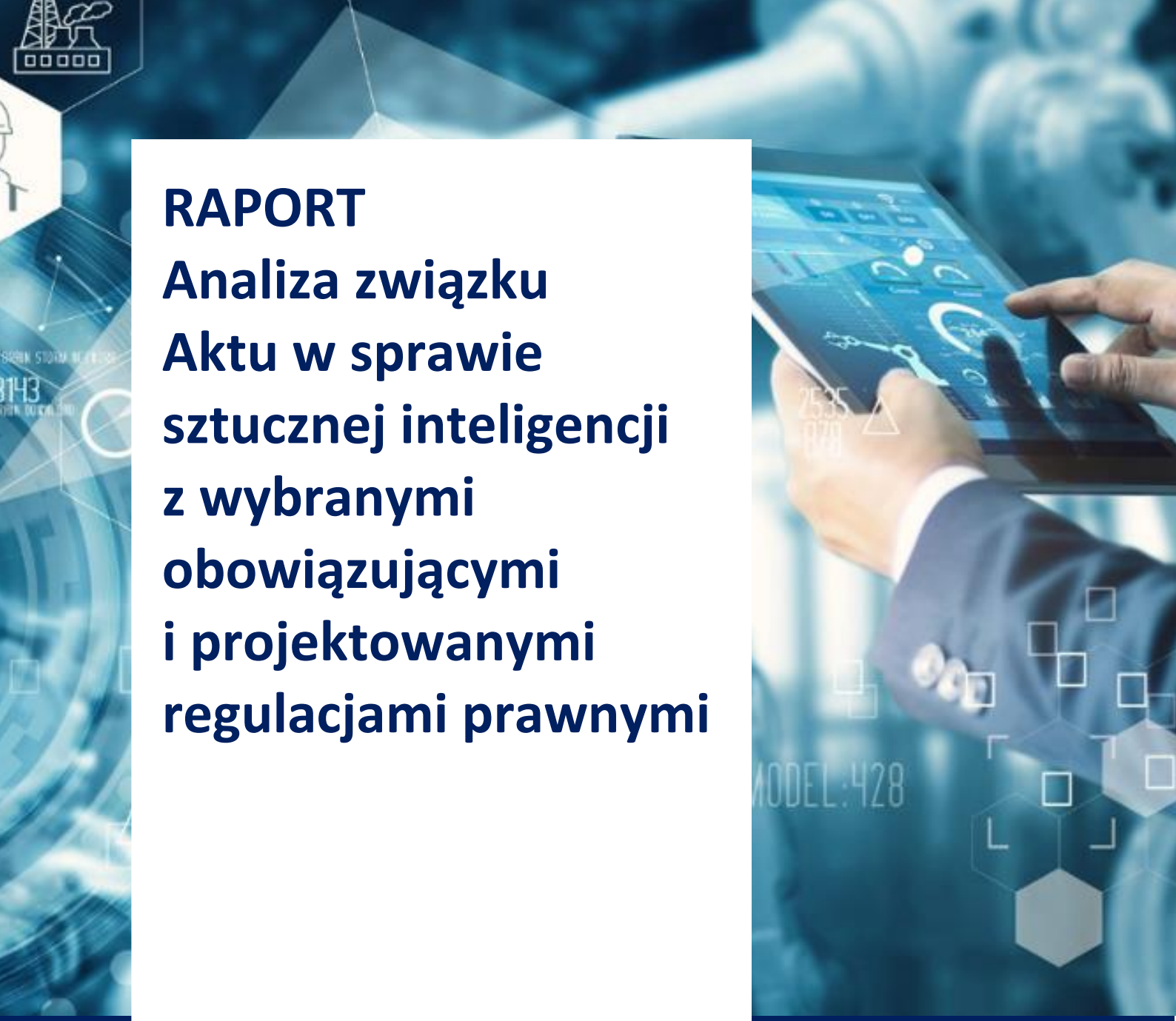

RAPORT
Analiza związku Aktu w sprawie sztucznej inteligencji z wybranymi obowiązującymi i projektowanymi regulacjami prawnymi

Raport przygotowany przez
Grupę Roboczą ds. Sztucznej Inteligencji
Podgrupa ds. etyki i prawa

Ministerstwo Cyfryzacji

GRAI
GRUPA ROBOCZA
DS. SZTUCZNEJ INTELIGENCJI

POGLĄDY WYRAŻONE W TYM DOKUMENCIE SĄ POGLĄDAMI ICH AUTORÓW I NIE MUSZĄ ODZWIERCIEDLAĆ STANOWISKA POLSKIEGO RZĄDU

Warszawa, sierpień 2023

Spis treści

Grupa robocza ds. etyki i prawa sztucznej inteligencji

Niniejszy raport przygotowany został przez podgrupę ds. etyki i prawa sztucznej inteligencji[1] działającej w ramach Grupy Roboczej ds. Sztucznej Inteligencji (GRAI) przy Ministrze Cyfryzacji.

Zasadniczym celem podgrupy jest wsparcie rozwoju polskiego ekosystemu sztucznej inteligencji w zakresie etyki i prawa.

Podgrupa robocza składa się z kilkudziesięciu ekspertów, specjalizujących się w różnych dziedzinach prawa, jak również osób zainteresowanych etycznym wymiarem sztucznej inteligencji. Eksperci posiadają doświadczenie zawodowe wyniesione z różnych branż i sektorów, w tym z działalności w zakresie doradztwa prawnego, sektora biznesowego, administracji i świata nauki.

Prace podgrupy ds. etyki i prawa sztucznej inteligencji obejmują między innymi następujące działania:

- prowadzenie analizy i przedstawianie rekomendacji dotyczących projektów aktów prawnych i innych dokumentów przedstawionych przez KPRM,
- wsparcie w zakresie ewaluacji i dalszego rozwoju Polityki rozwoju sztucznej inteligencji w Polsce,
- prowadzenie analiz i badań z zakresu prawnych i etycznych aspektów sztucznej inteligencji,
- wypracowywanie koncepcji i przedstawienia rekomendacji w kwestiach dotyczących rozwoju sztucznej inteligencji, w tym jej ram prawnych, zmian legislacyjnych oraz dobrych praktyk,
- wsparcie innych grup roboczych.

Niniejszy raport sporządzony został przez zespół w składzie:

- r.pr. Roman Bieda,
- adw. Michał Chodorek
- r.pr. Witold Chomiczewski
- adw. Hanna Jankowska
- adw. Alicja Kaszuba
- r.pr. Błażej Koczetkow
- dr Dominik Lubasz
- prokurator Andrzej Ludwiński
- dr hab. Monika Namysłowska, prof. UŁ
- r.pr. Aleksandra Piech
- Luiza Piskorek
- Dorota Skrodzka-Kwietniak
- Przemysław Sotowski
- r.pr. Monika Susałko
- dr Kamil Szpyt
- dr hab. Marek Świerczyński, prof. UKSW
- dr inż. Paweł Tadejko
- sędzia Konrad Wasik
- dr n. fiz. Magdalena Wicher
- Michał Włodczak

Pracami zespołu kierował r.pr. Roman Bieda – lider podgrupy roboczej ds. etyki i prawa sztucznej inteligencji.

Redakcja ze strony Ministerstwa Cyfryzacji:
Sylwia Stefaniak

[1] Szerzej na temat grupy zob. https://www.gov.pl/web/ai/podgrupa-ds-etyki-i-prawa

I. Zakres i cele analizy

W dniu 21 kwietnia 2021 r. Komisja Europejska przedstawiła wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii[2] (dalej: Akt w sprawie sztucznej inteligencji lub AI ACT lub AIA).

Tworzenie, rozwój i wykorzystanie systemów sztucznej inteligencji wymagało będzie jednak uwzględnienia nie tylko przepisów AI ACT, lecz także szeregu innych, istniejących i aktualnie projektowanych regulacji prawnych.

Głównym celem niniejszego raportu jest przedstawienie związku („mapowania") przepisów AI ACT z wybranymi obowiązującymi i projektowanymi krajowymi i europejskimi regulacjami prawnymi. W ramach analizy odnieśliśmy się również do wytycznych Urzędu Komisji Nadzoru Finansowego, mających znaczenie dla obszarów, w których sztuczna inteligencja może być lub jest wykorzystywana przez podmioty nadzorowane.

Analiza przeprowadzona została w oparciu o powyżej wskazany przedstawiony przez Komisję Europejską projekt AI ACT.

Raport nie obejmuje wyczerpującego przedstawienia relacji AI Act z obowiązującymi przepisami lub projektami aktów prawnych. W ramach przeprowadzonej analizy wskazaliśmy na zależności pomiędzy AIA i wybranymi aktami prawnymi, przepisami i projektami aktów prawnych.

Niniejszy raport stanowi wynik pierwszego etapu analizy. W ramach kolejnych działań zamierzamy prowadzić dalszą analizę relacji i związków pomiędzy AI Act i przedstawionymi w niniejszym raporcie aktami prawnymi/projektami, jak również prowadzić mapowanie kolejnych aktów prawnych.

Wyrażamy nadzieję, że niniejszy raport przyczyni się do budowania świadomości ram prawnych dla tworzenia i eksploatacji systemów sztucznej inteligencji. Raport jest wyłącznie wyrazem osobistych opinii jego autorów, nie stanowi natomiast opinii prawnej i nie może być podstawą jakichkolwiek decyzji, w szczególności – biznesowych.

[2] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206

II. Mapowanie Aktu w sprawie sztucznej inteligencji

1. Ogólne rozporządzenie o ochronie danych (RODO)

1.1 Wstęp

Jednym z zasadniczych zagadnień spójności systemowej regulacji dotyczącej sztucznej inteligencji jest zagadnienie spójności z przepisami RODO.

Celem projektodawcy unijnego zadeklarowanym w pkt 1.2 Explanatory Memorandum jest, by projektowany AI ACT miał jedynie uzupełniać RODO oraz dyrektywę 2016/680 o zestaw zharmonizowanych przepisów mających zastosowanie do projektowania, opracowywania i stosowania niektórych systemów SI wysokiego ryzyka oraz ograniczeń dotyczących niektórych zastosowań systemów zdalnej identyfikacji biometrycznej.

Wątpliwości co do rzeczywistych intencji powstają jednak już na gruncie analizy podstawy prawnej wydania Aktu w sprawie sztucznej inteligencji. Wskazano bowiem, że jest nią m.in. art. 16 TFUE[3] (ochrona danych osobowych) bez dalszego wyjaśnienia, czy to w motywach, czy w części normatywnej, relacji AIA do obowiązujących przepisów z zakresu ochrony danych osobowych.

Wątpliwe jest też, czy proponowane w Akcie w sprawie sztucznej inteligencji zakazy mogą odwoływać się do art. 16 ust. 2 TFUE. Projektowany katalog zakazanych działań nie jest bowiem bezpośrednio ukierunkowany na ochronę danych osobowych, lecz na inne prawa podstawowe i wolności.

Ponadto w motywie 41 AIA wyrażono intencję, że „Niniejszego rozporządzenia nie należy rozumieć jako ustanawiającego podstawę prawną przetwarzania danych osobowych, w tym w stosownych przypadkach szczególnych kategorii danych osobowych", co jednak nie jest zgodne z brzmieniem poszczególnych przepisów projektu rozporządzenia, który wprowadza podstawy przetwarzania danych (zob. art. 10 ust. 5 i art. 54, motyw 72 AIA).

W konsekwencji brakuje doprecyzowania w art. 1 lub art. 2 AIA, że prawodawstwo Unii w zakresie ochrony danych osobowych, w szczególności RODO, ma zastosowanie do przetwarzania danych osobowych objętego również zakresem Aktu w sprawie sztucznej inteligencji, a ponadto, że AIA nie stoi na przeszkodzie zmianom RODO.

Brak jest wyraźnego wskazania, że projektowane rozporządzenie nie wyłącza stosowania istniejących przepisów UE regulujących przetwarzanie danych, w tym w zakresie kompetencji właściwych organów nadzorczych.

Powyższe istotnie obniża skuteczność mapowania, którą pogłębia jeszcze obecna sprzeczność niektórych motywów i regulacji szczegółowej (motyw 41 i art. 10 ust. 5 i art. 54), a także pozór wyznaczania relacji w przepisach szczegółowych, o czym szerzej w tabeli.

Zastosowane mechanizmy regulacyjne, jak np. podejście oparte na ryzyku, które oddziaływać mogą na wyznaczenie wzajemnych interakcji pomiędzy RODO a AIA, również nie wykazują spójności. W ogólnym rozporządzeniu o ochronie danych analiza ryzyka nakierowana jest na weryfikację wpływu na prawa

[3] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A12012E%2FTXT

i wolności podmiotów danych, natomiast w AIA wprowadzono ujęcie produktowe, specyficznie ujęte poprzez odesłanie w art. 65 do art. 3 pkt 19 rozporządzenia 2019/1020 stanowiącego, że systemy sztucznej inteligencji stwarzające ryzyko rozumie się jako produkt stwarzający ryzyko w rozumieniu art. 3 pkt 19 rozporządzenia (UE) 2019/1020, o ile wspomniane ryzyko wiąże się z zagrożeniem dla zdrowia i bezpieczeństwa lub praw podstawowych obywateli. Oddziałuje to na przyjętą koncepcję regulacyjną kierowania zasadniczej części obowiązków prawnych do dostawców systemów SI i równoczesnego ograniczania obowiązków użytkowników w sposób potencjalnie kolidujących z RODO (art. 29 ust. 5 AIA).

Na brak kompleksowego uregulowania kwestii relacji Aktu w sprawie sztucznej inteligencji do przepisów nie tylko RODO, ale i np. konsumenckich, wskazywano w trakcie procesu legislacyjnego m.in. w opinii EIOD i EDPB[4].

1.2 Tabela porównawcza

Akt Prawny	**Ogólne rozporządzenie o ochronie danych**	
AIA	RODO	Opis
Art. 3 pkt 1)	Art. 4 pkt 4) i Art. 22	Systemy SI definiowane w art. 3 pkt 1) AIA w obszarze wykorzystującym dane osobowe realizować mogą operacje przetwarzania danych osobowych, w tym profilowanie w rozumieniu art. 4 pkt 4) RODO, oraz składające się na zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach w rozumieniu art. 22 RODO, powodując konieczność zastosowania odpowiednich regulacji RODO.
Art. 3 pkt 2)-4)	Art. 4 pkt 7)-8)	Podmiot zobowiązany, w tym dostawca, użytkownik może zostać równocześnie uznany za administratora lub podmiot przetwarzający w rozumieniu RODO (odpowiednio art. 4 pkt 7)-8) RODO), zależnie od realizowanych przez nich obowiązków w zakresie wyznaczania celu przetwarzania danych w poszczególnych fazach tworzenia i wykorzystywania systemów SI. W konsekwencji prowadzi to do nałożenia na nich także stosowanych obowiązków wynikających z RODO

[4] Zob. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en, Zobacz również: Analiza wybranych aspektów projektu aktu w sprawie sztucznej inteligencji, Fundacja AI LAW TECH (https://www.gov.pl/web/ai/prawo).

Art. 3 pkt 29)-32) oraz Art. 10	Art. 4 pkt 1)	Poszczególne kategorie danych, tj. począwszy od danych treningowych, poprzez dane walidacyjne, a skończywszy na danych testowych, choć nie zawierają referencji do pojęcia danych osobowych, mogą stanowić dane osobowe w rozumieniu art. 4 pkt 1 RODO. Powoduje to konieczność zastosowania przesłanek legalizacyjnych zależnych od wykorzystywanych kategorii danych osobowych odpowiednio z art. 6 lub 9 rozporządzenia 2016/679 oraz spełnienia pozostałych wymogów RODO.
Art. 3 pkt 33)	Art. 4 pkt 14)	W motywie 7 AIA podkreślana jest zgodność pojęcia danych biometrycznych stosowanego w AIA (art. 3 pkt 33) z pojęciem danych biometrycznych zdefiniowanym w art. 4 pkt 14 RODO oraz nie wskazuje się na obowiązek interpretacji tegoż pojęcia w sposób spójny z definicją zawartą w RODO.
Motyw 24	Art. 9 ust. 1	Zgodnie z motywem 24 AIA wszelkie przetwarzanie danych biometrycznych i innych danych osobowych związane ze stosowaniem systemów sztucznej inteligencji do identyfikacji biometrycznej, inne niż w związku z wykorzystywaniem systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa zgodnie z przepisami AIA, w tym w przypadku gdy systemy te są stosowane przez właściwe organy w przestrzeni publicznej do celów innych niż egzekwowanie prawa, powinno nadal spełniać wszystkie wymogi wynikające, stosownie do przypadku, z art. 9 ust. 1 RODO. Wskazać natomiast należy, że art. 9 ust. 1 RODO wprowadza zasadniczy zakaz przetwarzania danych osobowych szczególnych kategorii w tym danych biometrycznych w rozumieniu art. 4 pkt 14 RODO. Szczegółowe wymogi dopuszczenia przetwarzania takich danych wprowadza natomiast art. 9 ust. 2 RODO i do niego powinna następować referencja.
Art. 5 ust. 1 lit. d)	Art. 9 ust. 1	W zakresie wprowadzanego zakazu wykorzystania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa, zakresowo następuje zazębienie się zakazów przetwarzania danych biometrycznych służących do identyfikacji na podstawie art. 9 ust. 1 RODO.

Art. 10	Art. 5 ust. 1 lit. a), c) I d)	W art. 10 AIA wprowadzone zostają kryteria jakości danych, które w przypadku danych osobowych podlegają równocześnie zasadom wynikającym z art. 5 ust. 1 RODO, w szczególności zasadzie rzetelności, leżącej u podstaw podejścia antydyskryminacyjnego, zasady minimalizacji danych wyznaczającej ramy adekwatności oraz zasady prawidłowości wskazującej na konieczność zapewnienia by dane były pozbawione błędów.
Art. 10 ust. 5	Art. 9 ust. 2	Wbrew założeniu niekreowania nowych podstaw prawnych przetwarzania danych osobowych (motyw 41 AIA) projektodawca zdecydował się na zaproponowanie regulacji przesłanki legalizacyjnej przetwarzania danych szczególnych kategorii wskazanych w art. 9 ust. 1 RODO dla dostawców systemów SI jako administratorów w zakresie, w jakim jest to ściśle niezbędne do realizowanych przez nich celów zapewnienia monitorowania, wykrywania i korygowania tendencyjności systemów SI i wysokiego ryzyka.
Art. 29 ust. 6	Art. 35 ust. 1, ust. 3 i ust. 4	Zauważona została konieczność przeprowadzenia w odpowiednich przypadkach oceny skutków dla ochrony danych (art. 35 RODO) przez użytkowników systemów SI, jednakże wprowadzono ograniczenie, że ocenę taką dokonuje się na podstawie danych dostarczonych przez dostawcę wymaganych zgodnie z art. 13 AIA bez ich weryfikacji, co może istotnie ograniczyć zakres oceny skutków dla ochrony danych (DPIA), a tym samym może wpływać negatywnie na zakres zastosowania RODO.
Art. 52 ust. 2	Art. 5 ust. 1 pkt a), Art. 13, 14, Art. 22	Przejrzystość przetwarzania danych osobowych. Obowiązki w zakresie przejrzystości w odniesieniu do użytkowników systemów rozpoznawania emocji lub systemów kategoryzacji biometrycznej, rozszerzają obowiązki przejrzystości wymagane przepisami RODO w przypadku przetwarzania danych biometrycznych.
Art. 54	Art. 6 ust. 1 i Art. 9 ust. 2	Art. 54 AIA wprowadza podstawę prawną do przetwarzania w ramach piaskownicy regulacyjnej danych osobowych zebranych w innych celach, w celu opracowywania określonych systemów SI w interesie publicznym. Tym samym zrealizowane jest zamierzenie regulacyjne wyrażone w motywie 72 AIA.
Art. 59	Art. 51 i n	Może zaistnieć zależność w przypadku ostatecznego wyboru krajowego organu nadzorczego w postaci organu nadzoru z obszaru danych osobowych.

Art. 71 ust. 6	Art. 83 ust. 2	Możliwy jest zbieg sankcji z art. 71 AIA i art. 83 RODO. Należy przy tym zwrócić uwagę na istotne rozbieżności zakresowe co do okoliczności branych pod uwagę przy określaniu wysokości kary pieniężnej w obu regulacjach.
Motyw 72 oraz Art. 53	Art. 83 ust. 2 lit. k	W motywie 72 AIA wyrażono intencję, która nie znalazła odzwierciedlenia w części normatywnej projektu, ale może być odczytywana w kontekście art. 83 ust. 2 lit. k RODO, stanowiącego o obowiązku uwzględniania przez organ wszelkich okoliczności wpływających na wymiar kary w taki sposób, że przy podejmowaniu przez właściwe organy decyzji o ewentualnym nałożeniu administracyjnej kary pieniężnej należy uwzględnić postępowanie uczestników korzystających z piaskownicy regulacyjnej.

2. Rozporządzenie PE i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych (MDR).

2.1 Wstęp

System sztucznej inteligencji może stanowić wyrób medyczny albo może nie spełniać definicji wyrobu medycznego, lecz być wykorzystywany w kontekście medycznym.

Gdy system sztucznej inteligencji stanowi wyrób medyczny musi on spełniać wymogi regulacyjne wynikające zarówno z MDR jak i AIA. Co istotne interakcja wymogów regulacyjnych wynikających z MDR oraz AIA jest szczególnie głęboka i rozległa.

Przede wszystkim, co do zasady, ocena zgodności systemu sztucznej inteligencji będącego wyrobem medycznym z wymogami MDR dokonywana będzie z udziałem zewnętrznej jednostki notyfikowanej. Powoduje to, że system sztucznej inteligencji będący wyrobem medycznym automatycznie spełniać będzie definicję systemu sztucznej inteligencji wysokiego ryzyka – w związku z czym do takich systemów zastosowanie znajdą wszystkie wymogi regulacyjne dotyczące systemów SI wysokiego ryzyka.

Metodologie MDR i AIA w zakresie obowiązków, które zrealizować musi producent wyrobu medycznego czy dostawca systemu SI wysokiego ryzyka, są przy tym podobne – obie regulacje skupiają się na podobnych etapach cyklu życia produktu i regulują te obowiązki w podobny sposób.

W szczególności, regulacje MDR i AIA będą się na siebie nakładać w tak kluczowych obszarach jak:

- wymogi dot. jakości danych wykorzystywanych do trenowania, walidacji i testowania systemu SI;
- metodologia prowadzenia oceny działania / oceny klinicznej systemu SI;
- system zarządzania jakością;
- dokumentacja techniczna;

- bezpieczeństwo i przejrzystość działania, kontrola użytkowników nad działaniem systemu SI będącego wyrobem medycznym;
- cyberbezpieczeństwo i bezpieczeństwo danych;
- zarządzanie zmianą.

2.2 Tabela porównawcza

Akt Prawny	**Rozporządzenie PE i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych (MDR)**	
AIA	MDR	Opis
Art. 3 pkt 1 w zw. z Art. 6 pkt 1 lit. a AIA	Art. 2 MDR	Wyrób medyczny może być systemem SI
Art. 6, Zał. II AIA		Zakwalifikowanie wyrobów medycznych jako systemów SI wysokiego ryzyka. „Bez względu na to, czy system sztucznej inteligencji wprowadza się do obrotu lub oddaje do użytku niezależnie od produktów, o których mowa w lit. a) i b), taki system sztucznej inteligencji uznaje się za system wysokiego ryzyka, jeżeli spełnione są oba poniższe warunki: a) system sztucznej inteligencji jest przeznaczony do wykorzystywania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II lub sam jest takim produktem; b) produkt, którego związanym z bezpieczeństwem elementem jest system sztucznej inteligencji, lub sam system sztucznej inteligencji jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II – ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku.”
Art. 8 – 20 AIA	Art. 5, 10, 20 MDR	Przepisy AIA określają obligatoryjne wymogi dla systemów SI wysokiego ryzyka. Zaliczyć można do nich: 1. wymóg ustanowienia, wdrożenia, utrzymania systemu zarządzania ryzykiem; 2. określenie wymagań dla danych treningowych, walidacyjnych i testowych; 3. wymóg prowadzenia dokumentacji technicznej;

		4. wymóg prowadzenia rejestru zdarzeń; 5. obowiązek projektowania i tworzenia systemów przejrzystych; 6. obowiązek informacyjny; 7. wymóg sprawowania nadzoru przez człowieka; 8. wymóg dokładności, solidności i cyberbezpieczeństwa systemów. 9. wymóg ustanowienia, wdrożenia, utrzymania systemu zarządzania jakością. 10. wymóg spełnienia ogólnych wymogów dotyczących bezpieczeństwa i działania w korelacji z zał. I MDR. Analogiczne wymogi nakłada MDR na systemy SI będące wyrobami medycznymi.
Art. 9 AIA	Art.10, Zał. I MDR	System zarządzania ryzykiem. Zarówno MDR, jak i AI regulują obowiązki dot. wdrożenia systemu zarządzania ryzykiem jako ciągłego, iteracyjnego procesu realizowanego przez cały cykl życia systemu SI wysokiego ryzyka, wymagającego regularnej, systematycznej aktualizacji.
Art. 10 AIA	Art. 10, Zał. I MDR	Wymogi dot. danych treningowych. Zarówno MDR, jak i AI regulują obowiązki dot. odpowiedniej jakości danych treningowych i odpowiednich praktyk w zakresie zarządzania danymi.
Art. 16-29 AIA	Art. 10, Zał. I MDR, Zał. II MDR	Obowiązki dostawców systemów SI wysokiego ryzyka: Art. 16 AIA. Dostawcy systemów sztucznej inteligencji wysokiego ryzyka: a) zapewniają zgodność swoich systemów SI wysokiego ryzyka z wymogami AIA; b) posiadają system zarządzania jakością zgodny z art. 17 AIA; c) sporządzają dokumentację techniczną systemu SI wysokiego ryzyka; d) przechowują rejestry zdarzeń generowane automatycznie przez ich systemy SI wysokiego ryzyka, jeżeli znajdują się one pod ich kontrolą; e) zapewniają, aby system SI wysokiego ryzyka poddano odpowiedniej procedurze oceny zgodności przed wprowadzeniem go do obrotu lub oddaniem go do użytku;

		f) wypełniają obowiązki rejestracyjne, o których mowa w art. 51 AIA; g) podejmują niezbędne działania naprawcze, jeżeli system SI wysokiego ryzyka nie spełnia wymogów ustanowionych w rozdziale 2 niniejszego tytułu; h) informują właściwe organy krajowe państw członkowskich, w których udostępnili lub oddali do użytku system SI, oraz, w stosownych przypadkach, jednostkę notyfikowaną o niezgodności z wymogami i o wszelkich podjętych działaniach naprawczych; i) umieszczają oznakowanie CE w swoich systemach SI wysokiego ryzyka na potwierdzenie zgodności z niniejszym rozporządzeniem zgodnie z art. 49 AIA; j) wykazują, na żądanie właściwego organu krajowego, zgodność systemu SI wysokiego ryzyka z wymogami ustanowionymi w AIA Tytuł III rozdz. 2. Ogólne obowiązki producentów wyrobów medycznych: Art. 10 ust.1 MDR. Producenci wprowadzający wyroby do obrotu lub do używania zapewniają, by wyroby były projektowane i produkowane zgodnie z wymogami MDR. Art. 10 ust. 2 MDR. Producenci ustanawiają, dokumentują, wdrażają i utrzymują system zarządzania ryzykiem zgodny z opisem w załączniku I sekcja 3 MDR. Art. 10 ust. 3 MDR. Producenci prowadzą ocenę kliniczną zgodnie z wymogami określonymi w art. 61 i załączniku XIV MDR, w tym obserwacje kliniczne po wprowadzeniu do obrotu. Art. 10 ust. 9 MDR. (…) Producenci wyrobów innych niż badane wyroby ustanawiają, dokumentują, wdrażają, utrzymują, na bieżąco aktualizują i systematycznie ulepszają system zarządzania jakością w najskuteczniejszy sposób zapewniający zgodność z niniejszym rozporządzeniem oraz proporcjonalnie do klasy ryzyka i rodzaju wyrobu (...) Art. 10 ust. 10 MDR. Producenci wyrobów wdrażają i na bieżąco aktualizują system nadzoru po wprowadzeniu do obrotu zgodnie z art. 83 MDR.

		Art. 10 ust.11. Producenci zapewniają, by wyrobowi towarzyszyły informacje określone w załączniku I sekcja 23 MDR sporządzone w języku urzędowym lub językach urzędowych Unii, określonych przez państwo członkowskie, w którym udostępnia się wyrób użytkownikowi lub pacjentowi. Elementy umieszczone na etykiecie muszą być nieusuwalne, łatwe do odczytania i zrozumiałe dla przewidzianych użytkowników lub pacjentów. Załącznik I MDR (Ogólne wymogi dotyczące bezpieczeństwa i działania): 15. Wyroby z funkcją diagnostyczną lub pomiarową 15.1. Wyroby do diagnostyki i wyroby z funkcją pomiarową są projektowane i produkowane w taki sposób, aby zapewnić wystarczającą dokładność, precyzję i stabilność, odpowiadającą ich przewidzianemu zastosowaniu, w oparciu o odpowiednie metody naukowe i techniczne. Producent podaje granice dokładności. 15.2. Pomiary dokonywane przez wyroby z funkcją pomiarową są wyrażone w legalnych jednostkach miary zgodnie z przepisami dyrektywy Rady 80/181/EWG. 17. Elektroniczne systemy programowalne – wyroby zawierające elektroniczne systemy programowalne i oprogramowanie samo w sobie będące wyrobem 17.1. Wyroby, które zawierają elektroniczne systemy programowalne, w tym oprogramowanie, lub oprogramowanie, które samo w sobie jest wyrobem, projektuje się tak, aby zapewnić powtarzalność wyników, niezawodność i działanie zgodne z ich przewidzianym używaniem. Na wypadek stanu pojedynczego uszkodzenia podejmuje się odpowiednie środki w celu wyeliminowania lub ograniczenia w możliwie największym stopniu ryzyka lub zakłócenia działania będących jego następstwem. 17.2. W przypadku wyrobów zawierających oprogramowanie lub w przypadku oprogramowania, które samo w sobie jest wyrobem, takie oprogramowanie jest rozwijane i wytwarzane zgodnie z aktualnym stanem wiedzy oraz z uwzględnieniem zasad cyklu życia oprogramowania, zarządzania ryzykiem, w tym bezpieczeństwa informacji, weryfikacji i walidacji.

		17.3. Oprogramowanie, o którym mowa w niniejszej sekcji i które jest przeznaczone do stosowania w połączeniu z mobilnymi platformami obliczeniowymi, jest projektowane i produkowane z uwzględnieniem szczególnych właściwości takiej mobilnej platformy (np. rozmiaru i współczynnika kontrastu ekranu) oraz czynników zewnętrznych związanych z jej stosowaniem (środowisko zróżnicowane pod względem oświetlenia lub hałasu). 17.4. Producent określa minimalne wymogi dotyczące sprzętu, właściwości sieci informatycznej oraz środków bezpieczeństwa informatycznego, w tym ochrony przed nieupoważnionym dostępem, niezbędne do zgodnego z przeznaczeniem działania tego oprogramowania.
Art. 17 AIA	Art. 10 ust. 2, Zał. I sekcja 3 MDR	Obowiązek wprowadzenia systemu zarządzania jakością. Zarówno MDR, jak i AI regulują obowiązki dot. wdrożenia systemu zarządzania jakością. System ten dokumentuje się w systematyczny i uporządkowany sposób w formie pisemnych polityk, procedur i instrukcji.
Art. 18, Zał. IV AIA	Art. 10 ust. 4, Zał. II MDR	Dokumentacja techniczna. Zarówno MDR, jak i AI regulują obowiązki dot. sporządzenia dokumentacji technicznej systemu SI wysokiego ryzyka / systemu SI będącego wyrobem medycznym.
Art. 30 AIA	Art. 35 MDR	Organy notyfikujące. Każde państwo członkowskie wyznacza lub ustanawia organ notyfikujący odpowiedzialny za opracowanie i stosowanie procedur koniecznych do oceny, wyznaczania i notyfikowania jednostek oceniających zgodność oraz za ich monitorowanie.
Art. 31 AIA	Art. 38 MDR	Wniosek jednostki oceniającej zgodność. Wymogi formalne wniosku o notyfikację do organu nadzorczego.
Art. 32 AIA	Art. 42 MDR	Procedura notyfikacji. Państwa członkowskie notyfikują Komisji UE i pozostałym państwom członkowskim wyznaczone przez siebie jednostki oceniające zgodność, wykorzystując elektroniczne narzędzie do notyfikacji

		będące częścią bazy danych o jednostkach notyfikowanych („baza danych NANDO") opracowanej i zarządzanej przez Komisję Europejską.
Art. 33 AIA	Art. 36 MDR	Jednostki notyfikacyjne. Jednostki notyfikowane weryfikują zgodność systemu SI wysokiego ryzyka / systemu SI będącego wyrobem medycznym zgodnie z procedurami oceny zgodności.
Art. 34 AIA	Art. 37 MDR	Jednostki zależne i podwykonawcy. Jednostki notyfikowane ponoszą pełną odpowiedzialność za zadania wykonywane przez podwykonawców lub jednostki zależne bez względu na ich siedzibę.
Art. 35 AIA	Art. 43 MDR	Numery identyfikacyjne i wykaz jednostek notyfikowanych. Komisja UE nadaje jednostkom notyfikowanym numer identyfikacyjny. Każdej jednostce nadaje się jeden tego rodzaju numer, nawet jeżeli notyfikowano ją na podstawie kilku aktów Unii.
Art. 36 AIA	Art. 46 MDR	Zmiany w notyfikacjach. W przypadku, gdy organ notyfikujący podejrzewa lub otrzyma informację, że jednostka notyfikowana przestała spełniać wymogi określone w AIA lub nie wypełnia swoich obowiązków, organ ten niezwłocznie wszczyna postępowanie wyjaśniające w tej sprawie z zachowaniem największej staranności. Jeżeli organ notyfikujący dojdzie do wniosku, że jednostka notyfikowana będąca przedmiotem postępowania wyjaśniającego przestała spełniać wymogi lub nie wypełnia swoich obowiązków, organ ten, stosownie do przypadku, ogranicza, zawiesza lub cofa notyfikację, w zależności od wagi uchybienia. Organ notyfikujący niezwłocznie informuje również o tym fakcie Komisję UE i pozostałe państwa członkowskie.
Art. 37-38 AIA	Art. 47, 49 MDR	Inne przepisy dotyczące jednostek notyfikowanych. Kwestionowanie kompetencji jednostek oraz koordynacja jednostek notyfikowanych.
Art. 43 AIA	Art. 52 MDR	Ocena zgodności. Dostawca systemu SI wysokiego ryzyka przeprowadza ocenę zgodności systemu. W odniesieniu do systemów SI wysokiego ryzyka będących wyrobami medycznymi

		lub stanowiących element produktu będącego wyrobem medycznym, ocena zgodności musi uwzględniać nie tylko wymogi AIA, ale również MDR. Na potrzeby tej oceny jednostki notyfikowane, które notyfikowano zgodnie z MDR, są uprawnione do przeprowadzania kontroli zgodności systemów SI wysokiego ryzyka z wymogami ustanowionymi w AIA, o ile zgodność tych jednostek notyfikowanych z wymogami ustanowionymi w art. 33 ust. 4, 9 i art. 10 AIA została oceniona w kontekście procedury notyfikacyjnej przewidzianej w MDR. Jeżeli akty prawne wymienione w załączniku II sekcja A AIA zapewniają producentowi produktu możliwość zrezygnowania z oceny zgodności przeprowadzanej przez osobę trzecią, o ile zapewnił on zgodność ze wszystkimi normami zharmonizowanymi obejmującymi wszystkie stosowne wymogi, taki producent może skorzystać z tej możliwość wyłącznie w przypadku, gdy zapewnił również zgodność z normami zharmonizowanymi lub – w stosownych przypadkach – wspólnymi specyfikacjami, o których mowa w art. 41 AIA, obejmującymi wymogi ustanowione w rozdziale 2 AIA.
Art. 44 AIA	Art. 56 MDR	Certyfikaty – opis. Zgodnie z Art. 56 ust. 1 MDR certyfikaty wydawane przez jednostki notyfikowane zgodnie z załącznikami IX, X i XI MDR sporządzone są w języku urzędowym Unii określonym przez państwo członkowskie, w którym ustanowiona została jednostka notyfikowana, lub – w przypadku braku takiego określenia – w języku urzędowym Unii akceptowanym przez jednostkę notyfikowaną. Minimalny zakres treści certyfikatów określono w załączniku XII MDR.
Art. 47 AIA	Art. 59 MDR	Odstępstwo od procedury oceny zgodności. Art. 47 ust. 1 AIA Na zasadzie odstępstwa od art. 43 każdy organ nadzoru rynku może wydać zezwolenie na wprowadzenie do obrotu lub oddanie do użytku konkretnych systemów SI wysokiego ryzyka na terytorium danego państwa członkowskiego w związku z wystąpieniem nadzwyczajnych względów dotyczących bezpieczeństwa publicznego lub ochrony zdrowia i życia osób, ochrony środowiska i ochrony

		kluczowych aktywów przemysłowych i infrastrukturalnych. Wspomniane zezwolenie wydaje się na ograniczony okres na czas przeprowadzenia niezbędnych procedur oceny zgodności, a jego ważność wygasa po zakończeniu tych procedur. Dokłada się starań, aby procedury te ukończono bez zbędnej zwłoki. Art. 59 ust. 1 MDR W drodze odstępstwa od art. 52 MDR właściwy organ może – na należycie uzasadniony wniosek – pozwolić na wprowadzenie do obrotu lub do używania na terytorium danego państwa członkowskiego określonego wyrobu, w przypadku którego nie przeprowadzono procedur, o których mowa w tym artykule, ale którego używanie leży w interesie zdrowia publicznego lub bezpieczeństwa lub zdrowia pacjentów.
Art. 48 AIA	Art. 19, Zał. IV MDR	Deklaracja zgodności UE. Dostawca sporządza pisemną deklarację zgodności UE dla każdego systemu SI i przechowuje ją w celu jej udostępnienia właściwym organom krajowym przez okres 10 lat od dnia wprowadzenia systemu SI do obrotu lub oddania go do użytku.
Art. 49 AIA	Art. 20 MDR	Oznakowanie zgodności CE. Oznakowanie CE umieszcza się na systemie SI wysokiego ryzyka w sposób widoczny, czytelny i trwały.
Art. 61 AIA	Art. 83, 84 MDR	Obowiązek monitorowania systemu SI wysokiego ryzyka po wprowadzeniu do obrotu. Dostawcy ustanawiają i dokumentują system monitorowania po wprowadzeniu do obrotu w sposób proporcjonalny do charakteru technologii SI i ryzyka związanego ze stosowaniem danego systemu SI wysokiego ryzyka. W ramach systemu monitorowania po wprowadzeniu do obrotu w aktywny i systematyczny sposób gromadzi się, dokumentuje i analizuje stosowne dane przekazywane przez użytkowników lub gromadzone z innych źródeł dotyczące skuteczności działania systemów SI wysokiego ryzyka w całym cyklu ich życia, przy czym system ten zapewnia dostawcy możliwość

		oceny, czy systemy SI stale spełniają wymogi ustanowione w tytule III rozdział 2 AIA.
Art. 62 AIA	Art. 87 MDR	Zgłaszanie poważnych incydentów i nieprawidłowego działania. Dostawcy systemów SI wysokiego ryzyka wprowadzanych do obrotu w Unii zgłaszają wszelkie poważne incydenty związane z tymi systemami lub wszelkie przypadki nieprawidłowego działania tych systemów, które stanowią naruszenie obowiązków przewidzianych w prawie Unii mającym na celu ochronę praw podstawowych, organom nadzoru rynku państw członkowskich, w których doszło do danego incydentu lub naruszenia. Dostawca dokonuje takiego zgłoszenia niezwłocznie po ustaleniu związku przyczynowego między systemem SI a incydentem lub nieprawidłowym działaniem lub po potwierdzeniu dostatecznie wysokiego prawdopodobieństwa istnienia takiego związku, a każdym razie najpóźniej w terminie 15 dni od dnia powzięcia przez dostawców wiedzy o wystąpieniu poważnego incydentu lub nieprawidłowego działania.
Art. 63 AIA	Art. 92-94 MDR	Nadzór rynku i kontrola systemów sztucznej inteligencji na rynku UE – egzekwowanie przepisów.
Art. 65 AIA	Art. 95 MDR	Procedura postępowania z systemami SI stwarzającymi ryzyko. „Produkt stwarzający ryzyko” oznacza produkt mogący mieć niekorzystny wpływ na zdrowie i bezpieczeństwo osób w ujęciu ogólnym, zdrowie i bezpieczeństwo w miejscu pracy, ochronę konsumentów, środowiska, bezpieczeństwa publicznego i innych interesów publicznych chronionych przez obowiązujące unijne prawodawstwo harmonizacyjne, w stopniu wykraczającym poza wpływ uważany za uzasadniony i dopuszczalny w stosunku do zamierzonego celu produktu lub w zwykłych lub dających się racjonalnie przewidzieć warunkach używania produktu, w tym długości okresu jego używania oraz, w stosownych przypadkach, wymagań dotyczących oddania do użytku, instalacji i konserwacji (rozporządzenie UE 2019/1020).

Art. 70 AIA	Art. 109 MDR	Poufność. Właściwe organy krajowe i jednostki notyfikowane zaangażowane w stosowanie AIA przestrzegają zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań.
Art.71 AIA	Ustawa o wyrobach medycznych z dnia 7.04.2022 r. (Dz.U. 2022 poz. 974).	Przepisy karne. Państwa członkowskie przyjmują zgodnie z AIA przepisy dotyczące kar, w tym administracyjnych kar pieniężnych, mających zastosowanie w przypadku naruszeń AIA i podejmują wszelkie działania niezbędne do zapewnienia ich właściwego i skutecznego wdrożenia. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Uwzględniają one w szczególności interesy drobnych dostawców i przedsiębiorstw typu start-up oraz ich rentowność.

3. Akt w sprawie danych

3.1 Wstęp

W dniu 23 lutego 2022 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (dalej: DA).

W generalnym ujęciu celem DA jest „zapewnienie sprawiedliwego podziału wartości danych między podmiotami gospodarki opartej o dane oraz na ułatwianie dostępu do danych i ich wykorzystania[5].” Przewidziane w projekcie DA rozwiązania prawne wykorzystane mogą zostać w celu pozyskania danych na potrzeby trenowania systemów SI.

3.2 Tabela porównawcza

Akt Prawny	**Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych)**	
AIA	Akt w sprawie danych (DA)	Opis
Art. 3 pkt 29 – 33	Art. 2 pkt 1	DA zawiera bardzo szeroką definicję „danych”. Z kolei AIA definiuje pojęcia „dane treningowe”, „dane walidacyjne”, „dane testowe”, „dane wejściowe”, „dane biometryczne”. Każde z zdefiniowanych w AIA kategorii danych obejmować mogą dane w rozumieniu DA.
Art. 3 pkt 1	Art. 2 pkt 3	Zgodnie z art. 2 pkt 3 DA przez „powiązaną usługę” rozumie się „usługę cyfrową, w tym oprogramowanie, która jest zawarta w produkcie lub wzajemnie z nim połączona w taki sposób, że jej brak uniemożliwiłby produktowi wykonywanie jednej z jego funkcji”. Pojęcia to obejmować może również system SI w rozumieniu AIA.
Art. 3 pkt 1	Art. 2 pkt 4	Zgodnie z art. 2 pkt 4 DA pojęcie „wirtualni asystenci” oznacza „oprogramowanie, które może przetwarzać żądania, zadania lub pytania, w tym na podstawie dźwięku, pisma, gestów lub ruchów, oraz w oparciu o te żądania, zadania lub pytania zapewnia dostęp do usług własnych i usług osób

[5] Wniosek w sprawie rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych), COM(2022) 68 final.

		trzecich lub kontroluje urządzenia własne i urządzenia osób trzecich". Wirtualny asystent może stanowić czy obejmować system SI w rozumieniu AIA.
Cały akt	Cały DA, w szczególności Art. 5, Art. 6, Art. 8, Art.9, Art. 13	DA stwarza możliwości pozyskania danych na potrzeby trenowania systemów SI. Odbiorca danych musi uwzględnić wynikające z DA zasady udostępnienia danych (w tym ograniczenia dotyczące wykorzystania danych, warunki umowy o udostępnienie danych, kwestię wynagrodzenia).
Art. 3 pkt 29 – 32	Art. 35	Art. 35 DA przewiduje, iż prawo prawo sui generis przewidziane w art. 7 dyrektywy 96/9/WE nie ma zastosowania do baz danych zawierających dane pozyskane lub wygenerowane podczas korzystania z produktu lub powiązanej usługi. Wyłącznie to dotyczyć może również baz danych wykorzystywanych jako tzw. zbiory treningowe, testowe czy walidacyjne.

4. Projekt Dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję

4.1 Wstęp

Projekt Dyrektywy w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji ma na celu wyeliminowanie jednej z głównych przeszkód na drodze do korzystania ze sztucznej inteligencji, jaką jest problem z określeniem zasad odpowiedzialności za działanie systemów SI. W ocenie Komisji Europejskiej obowiązujące w krajach członkowskich przepisy dotyczące odpowiedzialności nie są dostosowane do rozpatrywania roszczeń z tytułu odpowiedzialności za szkody spowodowane przez produkty i usługi oparte na sztucznej inteligencji ze względu na konieczność udowodnienia bezprawnego zachowania lub zaniechania osoby, która spowodowała szkodę, co ze względu na cechy sztucznej inteligencji (złożoność, autonomia, brak przejrzystości), może być dla poszkodowanego zbyt trudne lub nadmiernie kosztowne.

W celu zniwelowania tych problemów Dyrektywa reguluje następujące kwestie:

a) ujawnianie dowodów dotyczących systemów SI wysokiego ryzyka, aby umożliwić powodowi uzasadnienie roszczenia odszkodowawczego opartego na zasadzie winy;
b) rozkład ciężaru dowodu w przypadkach pozaumownych roszczeń odszkodowawczych opartych na zasadzie winy z tytułu szkód spowodowanych przez system SI.

4.2 Tabela porównawcza

Akt Prawny	**Wniosek: Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję)**	
AIA	Projekt Dyrektywy	Opis
Art. 3, Art. 6	Art. 2 pkt 1)-4)	Definicje systemu SI, systemu SI wysokiego ryzyka, dostawcy i użytkownika znajdujące się w art. 2 Projektu Dyrektywy odwołują się do definicji zawartych w AIA w celu zapewnienia spójności.
Art 16, Art. 24, Art. 28, Art. 29	Art. 3	Dyrektywa wprowadza uprawnienie dla sądów do nakazania ujawnienia dowodów dotyczących konkretnego systemu SI potencjalnemu powodowi pod warunkiem, że wcześniej zwrócił się on z wnioskiem do dostawcy, osoby podlegającej obowiązkom dostawcy lub do użytkownika o ujawnienie istotnych dowodów, którymi te osoby dysponują, dotyczących konkretnego systemu SI wysokiego ryzyka, co do którego istnieje podejrzenie, że spowodował szkodę, a potencjalny powód spotkał się z odmową ujawnienia dowodów. Wniosek musi być poparty faktami i dowodami uprawdopodobniającymi roszczenie. Sądy, na wniosek powoda, będą uprawnione do zastosowania szczególnych środków w celu zabezpieczenia dowodów. Zakres ujawnianych informacji powinien być ograniczony do proporcjonalnych i niezbędnych do uzasadnienia roszczenia odszkodowawczego, uwzględniając tajemnicę przedsiębiorstwa. Od nakazu ujawnienia informacji będą przysługiwały środki ochrony prawnej pozwalające kwestionować nakaz. Niezastosowanie się do nakazu będzie skutkowało (wzruszalnym) domniemaniem braku zachowania należytej staranności.
Rozdział 2 i 3 Tytułu III	Art. 4	Art. 4 wprowadza wzruszalne domniemanie istnienia związku przyczynowego pomiędzy winą pozwanego a wynikiem uzyskanym przez system SI (lub jego brakiem) jeżeli: i. została wykazana wina pozwanego (lub zastosowano domniemanie), ii. w oparciu o okoliczności można uznać, że istnieje uzasadnione prawdopodobieństwo, iż wina wpłynęła na wynik uzyskany przez system SI (lub na fakt nieuzyskania wyniku), iii. powód wykazał, że szkoda została spowodowana wynikiem uzyskanym przez system SI.

		W przypadku roszczenia odszkodowawczego w stosunku do dostawcy systemu SI wysokiego ryzyka podlegającemu wymogom rozdziałów 2 i 3 Tytułu III AI ACT (lub osobie podlegającej obowiązkom dostawcy) wina zostanie udowodniona wyłącznie poprzez wykazanie, że którykolwiek z następujących wymogów nie został spełniony: a) system sztucznej inteligencji wykorzystuje techniki obejmujące trenowanie modeli z wykorzystaniem danych, które nie zostały opracowane na podstawie zbiorów danych treningowych, walidacyjnych i testowych spełniających kryteria jakościowe, o których mowa w (art. 10 ust. 2-4 aktu w sprawie AI); b) system sztucznej inteligencji nie został zaprojektowany i opracowany w sposób spełniający wymogi w zakresie przejrzystości określone w (art. 13 aktu w sprawie AI); c) system sztucznej inteligencji nie został zaprojektowany i opracowany w sposób umożliwiający osobom fizycznym jego skuteczne nadzorowanie w okresie wykorzystywania systemu sztucznej inteligencji zgodnie z (art. 14 aktu w sprawie AI); d) system sztucznej inteligencji nie został zaprojektowany i opracowany w sposób umożliwiający osiągnięcie, z uwagi na jego przeznaczenie, odpowiedniego poziomu dokładności, solidności i cyberbezpieczeństwa zgodnie z [art. 15 i art. 16 lit. a) aktu w sprawie AI] lub e) niezwłocznie nie podjęto niezbędnych działań naprawczych w celu zapewnienia zgodności systemu sztucznej inteligencji z obowiązkami określonymi w (tytule III rozdział 2 aktu w sprawie AI) lub, odpowiednio, w celu wycofania go z rynku lub wycofania go od użytkowników zgodnie z [art. 16 lit. g) i art. 21 aktu w sprawie AI]. W przypadku roszczenia przeciwko użytkownikowi systemu SI wysokiego ryzyka wina zostanie udowodniona poprzez wykazanie, że użytkownik: a) nie wywiązał się z obowiązku użytkowania lub monitorowania systemu sztucznej inteligencji zgodnie z załączoną instrukcją użytkowania lub, w stosownych przypadkach, z obowiązku wstrzymania lub przerwania jego użytkowania zgodnie z (art. 29 aktu w sprawie AI) lub b) wprowadził do systemu sztucznej inteligencji dane wejściowe, nad którymi sprawuje kontrolę i które nie są

		adekwatne w odniesieniu do przeznaczenia tego systemu w rozumieniu (art. 29 ust. 3 aktu). Domniemanie związku przyczynowego w przypadku roszczenia odszkodowawczego dotyczącego systemu SI wysokiego ryzyka nie będzie stosowane przez sąd, jeżeli pozwany wykaże, że powód może uzyskać względnie łatwy dostęp do dowodów i wiedzy eksperckiej wystarczających, by udowodnić związek przyczynowy pomiędzy winą a wynikiem systemu SI. Dla roszczeń odszkodowawczych dotyczących systemów SI niebędących systemami wysokiego ryzyka, domniemanie związku przyczynowego ma zastosowanie wyłącznie wówczas, gdy sąd uzna, że jego udowodnienie jest nadmiernie trudne. Gdy pozwanym jest osoba, która korzystała z systemu SI w ramach osobistej działalności pozazawodowej, domniemanie ma zastosowanie wyłącznie wówczas, gdy wpływała w istotny sposób na warunki działania systemu SI lub gdy miała taki obowiązek i tego nie uczyniła.

5. Ustawa o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079, dalej: „Nowa ustawa wdrożeniowa").

5.1 Wstęp

W motywie 163 Rezolucji Parlamentu Europejskiego z dnia 3 maja 2022 r. w sprawie sztucznej inteligencji w epoce cyfrowej (2020/2266(INI))[6] podkreślono potrzebę poprawy dostępu do środków finansowych, zwłaszcza dla MŚP, przedsiębiorstw typu start-up i scale-up.

Wsparciu ze środków publicznych mogą wymagać: organ notyfikujący, jednostka oceniająca zgodność, jednostka notyfikowana oraz operatorzy systemów sztucznej inteligencji (w szczególności – dostawcy).

Dostępne źródła wsparcia finansowego można podzielić na środki unijne, środki krajowe oraz inne źródła finansowania (np. Norweski Mechanizm Finansowy).

Aby skorzystać z odpowiedniego źródła finansowania, należy spełnić wymogi wynikające z określonych aktów prawnych oraz skonkretyzowane w zasadach danego wsparcia np. dokumentacji konkursowej.

5.2 Tabela porównawcza

Akt Prawny	**Ustawa o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 („Nowa ustawa wdrożeniowa")**	
AIA	Nowa ustawa wdrożeniowa	Opis

[6] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_PL.html

Art. 3 pkt 8, pkt 19, pkt 21, 22	Art. 1 ust. 1	Przepisy AIA definiują: • operatora (w tym dostawcę i użytkownika), • organ notyfikujący, • jednostkę oceniającą, • jednostkę notyfikowaną. Do tych podmiotów może mieć zastosowanie Nowa ustawa wdrożeniowa, jeśli będą starały się o dofinansowanie projektu ze środków unijnych.
Art. 3 pkt 8, pkt 19, pkt 21, 22	Art. 2 pkt 1 i pkt 34	Wymienione wyżej kategorie podmiotów w Nowej ustawie wdrożeniowej są określane jako: • wnioskodawca (złożył wniosek o dofinansowanie projektu), • beneficjenta (zawarł umowę o dofinansowanie projektu).
brak	Art. 2 pkt 30 Art. 5	Przepis definiuje „wytyczne” – wytyczne są skierowane do instytucji uczestniczących w realizacji programów operacyjnych np. ministerstw czy agencji wykonawczych, ale także do beneficjentów. Wytyczne mają zapewnić ujednolicone warunki i procedury. Realizacja projektu przez beneficjenta musi odbywać się zgodnie z wytycznymi, aby umowa o dofinansowanie mogła zostać uznana za prawidłowo zrealizowaną. Wszystkie podmioty starające się o dofinansowanie ze środków europejskich powinny zapoznać się z odpowiednimi wytycznymi Wytyczne są publikowane pod adresem https://www.gov.pl/web/fundusze-regiony/wytyczne
Art. 5 Art. 6 Art. 8 i nast. z rozdz. 2 i 3	Art. 22 ust. 1	Przepis wskazuje na czym polega kontrola i audyt programu operacyjnego. Służą one zapewnieniu, że system zarządzania i kontroli programu operacyjnego działa prawidłowo, a wydatki w ramach programu operacyjnego ponoszone są zgodnie z prawem oraz zasadami unijnymi i krajowymi. Przekłada się to na zasady zawierania i nadzoru nad wykonywaniem umów o dofinansowanie projektów. Kontrola realizacji umowy o dofinansowanie projektu może zatem dotyczyć stosowania zakazanych praktyk w zakresie sztucznej inteligencji oraz prawidłowej klasyfikacji systemów SI zgodnie z przyjętymi w AIA zasadami. W konsekwencji, kontrola systemów SI wysokiego ryzyka może dotyczyć zgodności z ustanowionymi w AIA wymogami.
Art. 33	Art. 2 pkt 1 i pkt 30	Jednostki notyfikowane mogą zostać wnioskodawcą/beneficjentem w zależności od zasad konkretnego dofinansowania.
Art. 53 ust. 1 i ust. 6 Art. 55	Art. 2 pkt 38 Art. 5	Tworzenie i finansowanie piaskownic regulacyjnych wymaga zgodności z przepisami AIA oraz może wymagać wydania nowych wytycznych w rozumieniu Nowej ustawy wdrożeniowej lub zmiany przyjętych wytycznych.

6. Prawo karne

6.1 Wstęp

Akt w sprawie sztucznej inteligencji reguluje kwestie związane z wykorzystaniem systemów SI na potrzeby postępowania karnego, gromadzenia dowodów i zapobiegania przestępczości. Porusza on także zagadnienie nielegalnego wykorzystania takich systemów oraz konieczność zapewnienia odpowiednich narzędzi do kontroli ich wykorzystania. Ma to wpływ na wskazane w poniższej tabeli obowiązujące przepisy.

Akt w sprawie sztucznej inteligencji z uwagi na szeroki zakres przedmiotowy, jaki obejmuje regulacja oraz wielowątkowość regulowanego zagadnienia przy uwzględnieniu obecnie już dość szerokiego wykorzystania technik informatycznych (w celu przede wszystkim identyfikacji i wykrywania sprawców przestępstw) dotychczas uregulowanych przepisami Kodeksu postępowania karnego, (ale także innych ustaw, w tym ustawy z dnia 6 kwietnia 1990 r. o Policji) pozostaje w bezpośrednim związku z przepisami prawa karnego procesowego, zaś pośrednio także prawa karnego materialnego.

Szczególny wpływ AIA widoczny jest przede wszystkim na polu przepisów dotyczących wykorzystania danych osobowych (zwłaszcza wizerunku osoby i danych biometrycznych) w celach związanych ze zwalczaniem i zapobieganiem przestępstw oraz wykrywaniem ich sprawców oraz zasadami wykorzystywania tych danych przez właściwe organy.

W związku z tym wprowadzenie AIA spowoduje konieczność dalszego dostosowania polskiego prawa. W obrębie przepisów dotyczących procesu karnego, konieczność ta spowodowana jest tym, że przepisy Kodeksu postępowania karnego obecnie nie regulują kwestii związanych z udostępnianiem danych biometrycznych oraz wykorzystaniem danych gromadzonych w toku postępowania przez systemy sztucznej inteligencji. Zasadne wydaje się również uregulowanie kwestii związanych z przechowywaniem rejestrów zdarzeń generowanych automatycznie przez dany system sztucznej inteligencji wysokiego ryzyka na potrzeby postępowań karnych oraz działań operacyjnych właściwych organów, w tym kwestie takie jak: okres retencji danych, organ uprawniony do ich żądania, forma decyzji w tym przedmiocie, przy czym niekoniecznie w ramach samego Kodeksu postępowania karnego. Na gruncie prawa karnego materialnego natomiast powstaje potrzeba rozważenia penalizacji naruszeń zasad wynikających z AI Akt, przy uwzględnieniu zasad skuteczności, proporcjonalności i odstraszania.

6.2 Tabela porównawcza

Akt Prawny	**Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U.2023.171 t.j) (dalej: Ustawa o Policji)**	
AIA	Ustawa o policji	Opis
Art. 5 (d), Art. 5 pkt 3, Art. 52	Art. 20	Art. 20 Ustawy o Policji, określa rodzaj i sposób wykorzystania danych osobowych do celów, o których mowa w art. 5d AIA. art. 5 pkt. 3 AIA – każde pojedyncze wykorzystanie systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa

		wymaga uzyskania uprzedniego zezwolenia udzielonego przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego, w którym ma nastąpić wykorzystanie, wydanego na uzasadniony wniosek i zgodnie ze szczegółowymi przepisami prawa krajowego, o których mowa w ust. 4. W należycie uzasadnionych nagłych przypadkach można jednak rozpocząć wykorzystywanie systemu bez zezwolenia, a o zezwolenie można wystąpić dopiero w trakcie lub po zakończeniu wykorzystywania Dodatkowo art. 52 AIA wskazuje na zniesienie rygorów określonych w art. 5 pkt 3 AIA odnośnie stosowania tzw. deepfake w przypadku, gdy korzystanie z takich rozwiązań zatwierdzono z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia dochodzeń/śledztw w związku z przestępstwami i ścigania ich sprawców lub gdy jest to konieczne do wykonywania prawa do wolności wypowiedzi i prawa do wolności sztuki i nauki zagwarantowanych w Karcie praw podstawowych Unii Europejskiej, z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich.
Akt Prawny	**Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2022 r. poz. 557 t.j.) (dalej: Ustawa o ABW)**	
AIA	Ustawa o ABW	Opis
Art. 5 (d), Art. 5 pkt 3,	Art. 23, 27-28b Ustawy o ABW	Przepisy art. 23, 27-28b ustawy o ABW dotyczą czynności operacyjno-rozpoznawczych realizowanych z wykorzystaniem środków technicznych, kontroli operacyjnej z wykorzystaniem takich środków oraz zasady uzyskiwania zgody organów na ich przeprowadzenie i sposób postępowania z materiałem tak uzyskanym – wykorzystanie systemów zdalnej identyfikacji biometrycznej
Akt Prawny	**Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz.U.2022.1375 t.j.) (dalej: KPK)**	
Art. 5 (d)	Art. 15 § 2 i 3	Przepis stanowi podstawę żądania na potrzeby postępowania karnego informacji znajdujących się w posiadaniu organów samorządowych i instytucji państwowych – tj. m.in. informacji, o których mowa w przepisie art. 15 § 2 KPK oraz 21 Ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości (DODO), a które na mocy wyjątku wskazanego w art. 5 d AIA mógłby zostać wykorzystane przez organy postępowania karnego przy użyciu systemów zdalnej identyfikacji

		biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa.
Art. 63 pkt 5	Art. 19 § 1 i 2	Art. 19 KPK przewiduje obowiązek informowania przez prokuratora i sąd o stwierdzonych naruszeniach w ich działaniu. Art. 63 pkt. 5 AIA przewiduje, że organy sprawujące nadzór nad organami ścigania mogą stanowić organ nadzoru rynku do celów AIA.
Art. 5 (d) (iii), Art. 52	Art. 74	Przepis art. 74 określa obowiązki udostępnienia przez podejrzanego (podejrzewanego) danych oraz środki służące egzekucji tych obowiązków. Wśród nich znajdują się również obowiązki dotyczące danych biometrycznych i poddania się procesowi ich pozyskiwania dla celów egzekwowania prawa, o których mowa w art. 5 (d) AIA.
Art. 5 (d)	Art. 168b	Nieuregulowana jest kwestia wykorzystania informacji uzyskanych w wyniku użycia systemów SI, o których mowa w art. 5 AIA jako dowodu w postępowaniu karnym, a bez której kwestia dopuszczalności ich wykorzystania w postępowaniu będzie wątpliwa.
Art. 5 (d) (iii)	Art. 192a § 1	Art. 192a KPK reguluje kwestie badań eliminacyjnych, do których wykorzystane mogą zostać systemy sztucznej inteligencji oraz sposób postępowania z materiałem niemającym już znaczenia dla postępowania – na co również kładzie nacisk AIA.
Art. 5 (d)	Art. 205 § 1	Przepis art. 205 KPK reguluje pozycję specjalisty w postępowaniu karnym. Wydaje się, że osoba obsługująca systemy SI wykorzystywane na potrzeby postępowania karnego powinna również zostać uwzględniona w tym przepisie.
Art. 5 (d),	Art. 218, 218a, 236a	W polskim prawie karnym nie została uregulowana kwestia udostępniania danych biometrycznych i innych wykorzystywanych dla potrzeb systemów SI. Brakuje również regulacji odnośnie formy żądania danych, organu uprawnionego (sąd, prokurator?) zakresu żądanych danych itp.
Art. 5 (d) (ii), Art. 5 pkt 3 i 4	Art. 241	Przepis reguluje kwestie kontroli operacyjnej oraz wykorzystania dowodów uzyskanych w ten sposób dla potrzeb postępowania karnego. AIA odwołuje się natomiast do wykorzystania systemów SI w celach prewencyjnych w związku z czym będzie to wykonywane w ramach kontroli operacyjnej, a także, zgodnie z art. 5 pkt 3 AIA – będzie wymagać zgody właściwego organu (sądu/prokuratora).

Art. 5	Art. 308	Brak w Kodeksie postępowania karnego odpowiednich przepisów określających zasady wykorzystania systemów, o których mowa w art. 5 (d) AIA w ramach tzw. czynności w niezbędnym zakresie.

7. Prawo cywilne (procesowe)

7.1 Wstęp.

AI Act jest aktem wielowątkowym o praktycznie nieograniczonym zasięgu, jeśli chodzi o powiązanie z poszczególnymi gałęziami prawa, a w tym także z prawem cywilnym procesowym. Algorytmy i nowoczesne narzędzia technologiczne mogą pomóc polskiemu wymiarowi sprawiedliwości pracować wydajniej i szybciej. Procesy w Polsce trwają latami, a tymczasem sztuczna inteligencja jest szansą na poprawę tej sytuacji. W tym kontekście uwypuklić należy kilka płaszczyzn, na których dochodzi do styku wymiaru sprawiedliwości i sztucznej inteligencji, a w konsekwencji związku AIA z przepisami prawa cywilnego procesowego.

Wskazać tutaj należy na instytucje uprawnienia sądu cywilnego dostępu do danych wygenerowanych przez systemy SI (art. 248 KPC), których użytkownikiem nie jest sąd (w tym choćby do rejestru zdarzeń), zapewnienia biegłym dostępu do systemu SI w razie potrzeby (art. 284 KPC, art. 293 KPC), wprowadzania do materiału dowodowego informacji uzyskanych od systemu SI (art. 309 KPC) i podstawy wyrokowania (art. 316 KPC). Dostosowania do AIA wymagają bowiem regulacje instytucji procesowych, które umożliwiałyby sądowi dostęp do systemów SI należących do podmiotów trzecich, a także informacji i dokumentów dotyczących systemu sztucznej inteligencji wysokiego ryzyka oraz kwestii współpracy z sądami cywilnymi przy wszelkich działaniach podejmowanych w odniesieniu do systemu sztucznej inteligencji wysokiego ryzyka i dostawców systemów sztucznej inteligencji wysokiego ryzyka, co stwarza konieczność rozważenia uzupełnienia kodeksu o te regulacje.

Po drugie, istnieje związek z AIA na płaszczyźnie wykorzystania systemów SI do rozpoznawania konkretnych spraw w postępowaniach sądowych o charakterze zinformatyzowanym, tj. postępowaniem wieczystoksięgowym, postępowaniem rejestrowym, europejskim postępowaniem nakazowym z rozporządzenia nr 1896/2006 Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. (Dz.Urz. UE L 399 z 30.12.2006, str. 1, z późn. zm.), elektronicznym postępowaniem upominawczym i postępowaniem przed sądem polubownym.

Po trzecie, sztuczna inteligencja może być skutecznie wykorzystywana przez wymiar sprawiedliwości. Systemy SI pomagać w analizie orzecznictwa, wykrywać trendy i linie orzecznicze w podobnych sprawach, przewidywać kierunek wyroku, analizować obszerne zbiory danych, czy choćby wyszukiwać normy prawne, które mogą mieć zastosowanie w konkretnej sprawie. Nie sposób w tym miejscu określić nawet ram prawa stosowanego w rozstrzyganiu spraw cywilnych, gospodarczych, pracowniczych, z ubezpieczeń społecznych, rodzinnych, wieczystoksięgowych itd., wymienić licznych linii orzeczniczych Sądu Najwyższego i poszczególnych sądów apelacyjnych, nie mówiąc już o orzecznictwie sądów okręgowych i rejonowych, niejednokrotnie odmiennie oceniających identyczne stany faktyczne. Każdy orzecznik wielokrotnie wylosował sprawę o identycznym stanie faktycznym, co sprawa prawomocnie rozstrzygnięta przez inny sąd. Zdarzają się nawet przypadki odmiennego rozstrzygania przez sędziów identycznych spraw w ramach tego samego wydziału sądu. Nie stanowi to

problemu, gdy powodem tego jest różna mentalność prawna sędziów. Problemem natomiast jest sytuacja, gdy sędziowie pozostają nieświadomi tego faktu. Systemy SI mogą okazać się nie tylko przydatne w zbieraniu materiału dowodowego, ale przede wszystkim mogą pomóc sędziemu zapoznać się z innymi podobnymi rozstrzygnięciami, powołaną argumentacją i pozwolić w ten sposób na szybkie podjęcie decyzji. Można wykorzystać w tym celu dostępną w Internecie bazę danych Portal Orzeczeń Sądów Powszechnych, w którym na dzień 4 marca 2023 r. znajdowało się 404 775 orzeczeń sądowych. Współczesny kodeks postępowania cywilnego nastawiony jest jednak w głównej mierze na tradycyjne postępowanie przed sądem bez udziału maszyn przy kształtowaniu orzeczenia kończącego postępowanie.

Tymczasem ustawodawca unijny wprost przewidział hipotetyczne zastosowanie systemu SI przy podejmowaniu przez sądy decyzji procesowych. Proponowane przez europejskiego ustawodawcę ramy prawne są kompleksowe i wprowadzają proporcjonalny system regulacyjny skoncentrowany wokół zdefiniowanego i opartego na analizie ryzyka podejścia regulacyjnego. Europejski prawodawca w AIA zaproponował bowiem rozdzielenie systemów sztucznej inteligencji wysokiego ryzyka od innych systemów sztucznej inteligencji. Za wysokie ryzyko uznaje się zgodnie z art. 6 ust. 2 w zw. z załącznikiem III pkt 8 systemu z obszaru sprawowania wymiaru sprawiedliwości i procesów demokratyczne, tj. systemy sztucznej inteligencji, które mają służyć organowi sądowemu pomocą w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego.

Należy dokonać ogólnego podziału prawniczej sztucznej inteligencji na dwie kategorie: systemów wyszukiwania prawa (ang. legal retrieval systems) i systemów analizy prawa (ang. legal analysis systems). Te pierwsze, w uproszczeniu, utożsamiać można z aktualnie występującymi na rynku komercyjnymi prawniczymi programami użytkowymi, na których pracują polscy sędziowie. Z kolei celem systemów analizy prawa jest określenie konsekwencji prawnych konkretnych okoliczności faktycznych. Wśród nich wyróżnić należy wspomniane maszyny wyrokujące oraz prawnicze systemy eksperckie (ang. legal expert systems). Z kolei te ostatnie dzielą się na oparte na regułach (ang. rule-based systems), bazujące na analizie przypadków (ang. case-based systems) i systemy hybrydowe (ang. hybrid systems). Systemów takich próżno szukać w codziennej pracy sędziego.

Tymczasem zgodnie z art. 6 ust. 2 AIA i punktem 8 lit. a) załącznika III za system sztucznej inteligencji wysokiego ryzyka uznaje się systemy sztucznej inteligencji, które mają służyć organowi sądowemu pomocą w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego. W przypadku wprowadzenia tego rodzaju systemu SI do polskiego porządku prawnego istnieje konieczność uregulowania podstaw jego stosowania w kontekście art. 316 KPC. Algorytmy sztucznej inteligencji mogą mieć zastosowanie przy przygotowywaniu dość standardowych części wyroków sądu, jak np. opisu dotyczącego stron postępowania, przebiegu postępowania wraz ze zwięzłym opisem stanowisk stron co do kluczowych dla sprawy kwestii spornych, podsumowaniem złożonych przez strony pism procesowych, prawa mającego zastosowanie do rozstrzygnięcia sprawy i kosztów postępowania. Rola sędziego mogłaby się sprowadzać do dokonania subsumpcji. Uwolniony w ten sposób czas sędziego mógłby zostać poświęcony na zajęcie się bardziej skomplikowanymi elementami rozpoznawania sporu, zarówno szybciej, jak i zapewne z uważniejszym przeanalizowaniem przytaczanych argumentów.

7.2 Tabela porównawcza

Akt Prawny	Kodeks postępowania cywilnego	
AIA	KPC	Opis
Art. 3 pkt 1) Art. 5 Art. 12 Art. 64	Art. 248	Ustawodawca unijny nie uregulował kwestii szczególnego trybu dostępu dla sądu do danych wypracowanych przez systemy SI. Tymczasem przepis art. 248 KPC wprowadza obowiązek przedstawienia na zarządzenie sądu dokumentu w rozumieniu art. 77(3) KC (pojęcie dokumentu jest szerokie i jest nim każdy nośnik informacji umożliwiający zapoznanie się z jej treścią). Wykorzystywanie systemów SI wraz z ich szczególnymi cechami (np. efekt czarnej skrzynki, złożoność, zależność od danych, autonomiczne zachowanie) może mieć negatywny wpływ na szereg praw podstawowych. Niezależnie od tego, że AIA zmierza do zapewnienia wysokiego poziomu ochrony praw podstawowych i minimalizacji ryzyka błędnych lub stronniczych decyzji podejmowanych przy wsparciu systemów SI, to istotnym jest zapewnienie sądom cywilnym dostępu do danych wypracowanych przez systemy sztucznej inteligencji, w tym przez systemy wykorzystania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym". Brak jest regulacji kwestii związanych z udostępnianiem takich danych na potrzeby sądu cywilnego, a także informacji i dokumentów niezbędnych do wykazania zgodności systemu sztucznej inteligencji wysokiego ryzyka oraz kwestii współpracy z sądami cywilnymi w odniesieniu do systemu sztucznej inteligencji wysokiego ryzyka, dostawców systemów, upoważnionych przedstawicieli i użytkowników, co stwarza konieczność uzupełnienia kodeksu o te regulacje. Pozostaje to w związku z art. 3 ust. 1 i art. 5 AIA. Powstaje także związek stosowania art. 248 KPC w zw. z art. 12 AIA w zakresie dostępu sądu cywilnego do rejestrów zdarzeń. Nieuregulowana jest także kwestia dostępu sądów do dokumentacji sporządzonej lub prowadzonej na podstawie rozporządzenia AIA, którą przewidziano w art. 64 ust. 3 AIA.

Art. 3 pkt) 1 Art. 5	Art. 254	Przepis art. 254 KPC określa zasady badania przez sąd prawdziwości dokumentu, w tym udostępnienia informatycznego nośnika danych. Sąd w razie potrzeby może wezwać wystawcę dokumentu sporządzonego w postaci elektronicznej do udostępnienia informatycznego nośnika danych, na którym ten dokument został zapisany. Należy rozważyć, czy za nośnik może być uznany cały system sztucznej inteligencji, a nie tylko wypracowane przez niego dane. Brak jest regulacji przewidującej sposób dostępu do nośnika danych będących systemem SI. Powstaje zatem związek między art. 248 i art. 254 KPC z przepisami art. 3 ust. 1 i art. 5 AIA.
Art. 12 Art. 64 ust. 3	Art. 284 Art. 293 Art. 294	Przepis art. 284 KPC określa zarządzenia sądu zmierzające do zapewnienia biegłemu prawidłowego przygotowania opinii sądowej. Należy rozważyć uzupełnienie regulacji o sposób i tryb (choćby w formie rozporządzenia wydanego na podstawie delegacji w KPC) dostępu biegłego sądowego do dokumentacji sporządzonej lub prowadzonej na podstawie AIA, a także kodu źródłowego systemu sztucznej inteligencji na potrzeby związane z postępowaniem cywilnym.
Art. 3 pkt) 1 i Art. 5	Art. 309	Artykuł 309 KPC przewiduje możliwość dopuszczenia i przeprowadzenia innych środków dowodowych, nienazwanych w ustawie, przy odpowiednim zastosowaniu przepisów o dowodach. Brak jest aktualnie regulacji przewidującej tryb i sposób wykorzystania systemów SI w postępowaniu dowodowym w charakterze źródła dowodowego (np. świadka). Jakkolwiek wydawać się to może absurdalne, to zaznaczyć należy, że towarzyszące człowiekowi maszyny cyfrowe, a więc maszyny z własną pamięcią i mocą obliczeniową, wyposażone w odpowiednie urządzenia, nie potrzebują przy odpowiedniej konfiguracji ludzi, aby obserwować świat (Alexa, Siri). Nie wszystkie dane cyfrowe istnieją wskutek wprowadzenia ich przez człowieka do pamięci maszyny cyfrowej. Stąd powstaje problem wprowadzenia do materiału dowodowego danych uzyskanych przez system SI[7], czy dostępu do danych wypracowanych w ramach Internetu rzeczy, np. kamer monitoringu miejskiego, danych diagnostycznych z autonomicznych samochodów.

[7] https://assets.documentcloud.org/documents/5113287/Timothy-Verrill-order-for-Amazon-Echo-data.pdf; zob. I.A. Hamilton, *A judge has ordered Amazon to hand over recordings from an Echo to help solve a double murder case* https://www.businessinsider.com/amazon-ordered-to-disclose-echo-alexa-recordings-murder-case-2018-11

Art. 6 ust. 2 w zw. z punktem 8 lit. a) załącznika III	Art. 316	Przepis art. 316 KPC określa jaki stan rzeczy, który sąd bierze pod uwagę przy wyrokowaniu. Tymczasem zgodnie z art. 6 ust. 2 AIA i punktem 8 lit. a) załącznika III za system sztucznej inteligencji wysokiego ryzyka uznaje się systemy sztucznej inteligencji, które mają służyć organowi sądowemu pomocą w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego. W przypadku wprowadzenia tego rodzaju systemu SI do polskiego porządku prawnego istnieje konieczność uregulowania podstaw jego stosowania w kontekście art. 316 KPC. Algorytmy sztucznej inteligencji mogą mieć zastosowanie przy przygotowywaniu dość standardowych części wyroków sądu, jak np. opisu dotyczącego stron postępowania, przebiegu postępowania wraz ze zwięzłym opisem stanowisk stron co do kluczowych dla sprawy kwestii spornych, podsumowaniem złożonych przez strony pism procesowych, prawa mającego zastosowanie do rozstrzygnięcia sprawy i kosztów postępowania. Rola sędziego mogłaby się sprowadzać do dokonania subsumpcji. Uwolniony w ten sposób czas sędziego mógłby zostać poświęcony na zajęcie się bardziej skomplikowanymi elementami rozpoznawania sporu, zarówno szybciej, jak i zapewne z uważniejszym przeanalizowaniem przytaczanych argumentów.
Art. 3 pkt 1) w zw. z załącznikiem I Art. 5	Art. 505(15)	Art. 505(15) KPC reguluje postępowanie w sprawach transgranicznych, tzw. europejskie postępowanie nakazowe, uregulowane w rozporządzeniu (WE) nr 1896/2006 Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. ustanawiającego postępowanie w sprawie europejskiego nakazu zapłaty (Dz.Urz. UE L 399 z 30.12.2006, str. 1, z późn. zm.) W art. 8 zd. 2 rozporządzenia 1896/2006 ustawodawca unijny dopuścił możliwość automatycznego badania pozwu. Hipotetycznie dopuszczono możliwość wydawania w postępowaniu cywilnym rozstrzygnięć bez udziału człowieka. Norma ta jest fakultatywna dla państw członkowskich, a polski ustawodawca nie zdecydował się na automatyzację europejskiego postępowania nakazowego. Istnieje jednak możliwość takiego ukształtowania postępowania z art. 505(15) KPC, że dojdzie do udziału systemu SI w polskim postępowaniu cywilnym. Zaznaczyć należy, że ustawodawca unijny (motyw 11) wprost zaakcentował, że postępowanie w sprawie europejskiego

		nakazu zapłaty powinno umożliwiać wykorzystanie automatycznego przetwarzania danych.
Art. 3 pkt 1) w zw. z załącznikiem I Art. 5	Art. 505(28) Art. 505(29) Art. 505(30) Art. 505(31)	Elektroniczne postępowanie upominawcze ma na celu usprawnienie rozpoznawania drobnych spraw cywilnych poprzez powiązanie tradycyjnego modelu postępowania upominawczego z możliwościami wynikającymi z zastosowania nowoczesnych rozwiązań technologicznych. EPU jest zinformatyzowanym postępowaniem cywilnym, w którym zdecydowana większość czynności dokonywana jest elektronicznie, a w tym dotyczy to czynności sądu i referendarza sądowego. Polski ustawodawca nie zdecydował się na wyłączenie udziału człowieka (analogicznie, jak funkcjonujące w Wielkiej Brytanii, ang. Money Claim Online) i wprowadzenie automatyzacji w podejmowaniu niektórych decyzji (tak jak w Niemczech niem. automatisertes Mahnverfahren). Na chwilę obecną system informatyczny obsługujący EPU nie jest systemem sztucznej inteligencji w rozumieniu art. 3 pkt 1) AIA, gdyż nie jest opracowany przy użyciu jednej spośród technik i podejść wymienionych w załączniku I. Charakteryzuje się jedynie automatycznym przetwarzaniem danych, wyrażającym się w zasadzie w samoistnym kopiowaniu informacji pomiędzy pismami procesowymi i sądowymi, możliwe i celowe wydaje się redefiniowanie systemu w kierunku systemu ekspertowego badającego co najmniej automatycznie warunki formalne pozwu (art. 505(32) KPC) i wymagalność roszczenia (art. 505(29) KPC) bez udziału czynnika ludzkiego. Wzorem mógłby być tu art. 14 § 1b KPA, dodany ustawą z dnia 18.11.2020 r. (Dz.U. z 2020 r. poz. 2320 ze zm. z Dz.U. z 2021 r. poz. 1135), która weszła w życie 5.10.2021 r., przewidujący autonomiczne działanie systemu i generowanie pism w postępowaniu administracyjnym. Powyższe mogłoby nastąpić z poszanowaniem art. 22 RODO. Należy postulować udoskonalenie elektronicznego postępowania upominawczego w kierunku systemu SI opartego o mechanizm uczenia maszynowego nadzorowanego przez człowieka, biorąc pod uwagę, że wydanie orzeczenia w elektronicznym postępowaniu upominawczym następuje bez badania dowodów.

Art. 3 pkt 1) w zw. z załącznikiem I Art. 5	Art. 626(1) KPC w zw. z Art. 1 i 36(3) ust. 1 ustawy o księgach wieczystych i hipotece tj. z dnia 22 lipca 2022 r. (Dz.U. z 2022 r. poz. 1728)	Sprawy w postępowaniu wieczystoksięgowym rozpoznają sądy poprzez dokonywanie wpisów w centralnej bazie danych. W ostatnim czasie Polska poczyniła postępy w dziedzinie zastosowania technologii informatycznych w postępowaniu wieczystoksięgowym. Z art. 36(3) u.k.w.h. wynika, że Minister Sprawiedliwości utrzymuje centralną bazę danych ksiąg wieczystych stanowiącą ogólnokrajowy zbiór ksiąg wieczystych prowadzonych w systemie teleinformatycznym. Jednocześnie w związku z dynamicznym rozwojem inicjatyw służących wykorzystaniu technologii łańcucha bloków (zapewnienie wiarygodności transakcji) oraz postępującą informatyzacją postępowania w sektorze obrotu nieruchomościami istnieje potrzeba analizy wpływu technologii blockchain na usprawnienie transakcji na rynku nieruchomości oraz procedury rejestracji. W tym kontekście postępowanie wieczystoksięgowe może pozostawiać w pośrednim związku z art. 3 pkt 1) w zw. z załącznikiem I oraz art. 5 AIA.
Art. 3 pkt 1) w zw. z załącznikiem I Art. 5	Art. 694 (1) i nast. KPC w zw. z Art. 1 ust. 1 i 2, Art. 3a ust. 1 ustawy o Krajowym Rejestrze Sądowym tj. z dnia 23 czerwca 2022 r. (Dz.U. z 2022 r. poz. 1683)	Sprawy w postępowaniu rejestrowym odbywają się za pośrednictwem systemu teleinformatycznego. W zakresie uregulowanym w art. 694(2a) KPC wszelkie czynności sądu utrwalane są wyłącznie w tym systemie. W zakresie postępowania rejestrowego poczynić należy tożsame uwagi jak w przypadku postępowania wieczystoksięgowego.
Art. 3 pkt 1) w zw. z załącznikiem I Art. 5	Art. 1165 Art. 1170 § 1 Art. 117, Art. 1174 Art. 1197 § 2 Art. 1206 § 1 pkt 1 Art. 1214 § 3 pkt 2 Art. 1215 § 2	Aktualnie postępowanie przed sądem polubownym ma charakter tradycyjny, zaś arbitrem może być wyłącznie osoba fizyczna (art. 1170 § 1 KPC). Pojawiają się jednak koncepcje o możliwości wykorzystywania przez sądy polubowne systemów SI.[8] Po pierwsze algorytmy sztucznej inteligencji mogą stanowić istotne ułatwienie zarówno dla stron postępowania, jak i dla pełnomocników stron. Możliwość analizy dużej ilości danych i skonfrontowanie ich z wyrokami wydanymi w przeszłości np. w ramach danej instytucji arbitrażowej lub przez danego arbitra może pomóc nie tylko

[8]Szerzej zob. L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, rozdział XIX.

		w wyborze przez stronę odpowiadającego jej arbitra, ale także w przewidzeniu kosztów, czasu trwania i wyniku postępowania arbitrażowego. Dostęp do tego rodzaju analiz może także pomóc stronom i pełnomocnikom w podjęciu decyzji co do najlepszego w danej sytuacji sposobu rozwiązania sporu, gdyż może się okazać, że korzystniej byłoby w konkretnym stanie faktycznym skorzystać np. z postępowania przed sądem powszechnym lub z mediacji. Natomiast w arbitrażu międzynarodowym konieczne jest przeszukiwanie dużych zbiorów danych dotyczących interpretacji poszczególnych przepisów, w tym częstokroć obszernego orzecznictwa nie tylko co do arbitrażowych kwestii proceduralnych, ale także w stosunku do prawa materialnego, często obcego. Zadania te tradycyjnie były wykonywane przez młodszych prawników. Algorytmy sztucznej inteligencji mogą zostać wykorzystane do szybszego i dokładniejszego wykonywania takich zadań odciążając prawników.

8. Prawo rynku kapitałowego, finansowego, ubezpieczeniowego

8.1 Wstęp

Zaufanie do rynku kapitałowego jest w znacznej mierze zależne od pewności w odniesieniu do otoczenia regulacyjnego i nadzorczego. Aby Polska mogła konkurować z najlepiej rozwiniętymi gospodarkami na świecie, musi ona stać się liderem w rozwoju technologii. Przyczynić się to powinno do podnoszenia wydajności i obniżania kosztów jednostkowych. Żeby to osiągnąć, technologia musi być wspierana przez odpowiednio powiązane ramy prawne, podatkowe i edukacyjne ułatwiające rozwój sektora FinTech i InsurTech. Konieczna jest eliminacja barier ograniczających możliwość podejmowania takiej działalności przez instytucje ryku kapitałowego i zachęcanie ich do działań innowacyjnych. Cel ten można osiągnąć między inny poprzez znaczące wykorzystanie procesów prawnych i regulacyjnych, e-administracji oraz tworzenie perspektywicznych rozwiązań FinTech, PayTech i InsurTech.

Polski rynek kapitałowy potrzebuje przewidywalnego, probiznesowego środowiska prawnego, które będzie ułatwiało inwestowanie i pozyskiwanie kapitału, zapewniało najwyższą ochronę inwestorom i usuwało przeszkody w dostępie do najwyższej jakości usług. Niezbędna jest transparentna komunikacja z zainteresowanymi stronami, w tym aktywne wykorzystanie oficjalnych rekomendacji i wytycznych dostępnych dla całego rynku, w celu ujednolicenia interpretacji przepisów i praktyk nadzorczych.

Wejście w życie Aktu w sprawie sztucznej inteligencji, który regulować będzie zagadnienia związane ze świadczeniem usług przez instytucje rynku kapitałowego może mieć wpływ na aktualność niektórych fragmentów publikacji UKNF, w szczególności w sytuacji istnienia przepisów wprost dotyczących danej formy aktywności uczestników rynku. W związku z powyższym wystąpić może konieczność publikacji

kolejnych stanowisk organu nadzoru, które regulować będą zagadnienia związane z wykorzystaniem przez rynek kapitałowy narzędzi AI.

Biorąc pod uwagę podnoszoną przez podmioty rynku kwestię złożoności wymagań regulacyjnych w zakresie usług inwestycyjnych, które jednocześnie mogą stanowić bariery wejścia na rynek lub ograniczające konkurencję, konieczne są działania zmierzające do budowy przyjaznego środowiska regulacyjnego dla podmiotów starających się wprowadzać na rynek innowacyjne rozwiązania i nowe technologie, mogące doprowadzić do zwiększenia poziomu aktywności inwestycyjnej w Polsce i zagwarantować przewagę konkurencyjną polskich podmiotów wobec odpowiedników z państw UE. Konieczne wydaje się wprowadzenie przez KNF tzw. piaskownicy regulacyjnej dla podmiotów typu FinTech i InsureTech. Działania podejmowane w ramach „piaskownicy regulacyjnej" powinny skutkować sprawną współpracą pomiędzy KNF i użytkownikami.

8.2 Rozporządzenie delegowane Komisji (UE) 2017/565 z dnia 25 kwietnia 2016 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy

Tabela porównawcza

Akt Prawny	**Rozporządzenie delegowane Komisji (UE) 2017/565 z dnia 25 kwietnia 2016 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy**	
AIA	Rozporządzenie delegowane Komisji (UE) 2017/565	Opis
Art. 3 pkt 1	Art. 54 ust. 1 akapit 2	W przypadku, gdy usługi doradztwa inwestycyjnego lub zarządzania portfelem są świadczone w całości lub w części poprzez zautomatyzowany lub na wpół zautomatyzowany system, odpowiedzialność za dokonanie oceny odpowiedniości spoczywa na firmie inwestycyjnej świadczącej usługę i nie może być zmniejszona poprzez użycie systemu elektronicznego przy dokonywaniu osobistej rekomendacji lub decyzji o przystąpieniu do transakcji. System, o którym mowa w art. 54 może być systemem sztucznej inteligencji.

8.3 Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2022r. poz. 1500 z późn. zm.; dalej ustawa o obrocie)

Tabela porównawcza

Akt Prawny	**Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2022r. poz. 1500 z późn. zm.; dalej ustawa o obrocie)**	
AIA	Ustawa o obrocie	Opis
Art. 3 pkt 1	Art. 3 pkt 2b	Handel algorytmiczny może wykorzystywać system sztucznej inteligencji.
Art. 3 pkt 1	Art. 3 pkt 2c	Technika handlu algorytmicznego o wysokiej częstotliwości może wykorzystywać system sztucznej inteligencji.
Art. 15	Art. 18 ust. 1 pkt 2	Obowiązek zapewnienia bezpiecznego i sprawnego przebiegu transakcji przez podmioty prowadzące rynek regulowany.
Art. 15	Art. 29d	Spółka prowadząca rynek regulowany zapewnia ochronę przed nieuprawnionym dostępem do systemu informatycznego, w którym przechowywane są dane osobowe.
Art. 15	Art. 74e	Firma inwestycyjna nabywająca lub zbywająca instrumenty finansowe przy wykorzystywaniu handlu algorytmicznego opracowuje, wdraża i stosuje adekwatne oraz skuteczne rozwiązania mające na celu: 1) zapewnienie odporności i wydajności urządzeń i systemów teleinformatycznych w stopniu odpowiadającym skali prowadzonej działalności, w szczególności limitom i progom transakcyjnym; 2) zapobieżenie nieprawidłowemu wpływowi urządzeń i systemów teleinformatycznych na sprawny i bezpieczny obrót instrumentami finansowymi, w szczególności przez kierowanie błędnych zleceń; 3) uniemożliwienie wykorzystania urządzeń i systemów teleinformatycznych w sposób naruszający przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylającego dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE lub regulacje systemów obrotu instrumentami finansowymi; 4) zapewnienie ciągłości obsługi oraz pracy urządzeń i systemów teleinformatycznych wykorzystywanych w prowadzonej działalności.

		Ponadto firma inwestycyjna monitoruje działanie urządzeń i systemów teleinformatycznych i przeprowadza testy w zakresie oceny prawidłowości ich działania w celu identyfikowania i eliminacji potencjalnych lub rzeczywistych naruszeń wymogów, o których mowa powyżej.
Art. 15	Art. 78 ust. 1 pkt 2	Obowiązek zapewnienia bezpiecznego i sprawnego przebiegu transakcji przez podmioty prowadzące alternatywny system obrotu.
Art. 15	Art. 78 ust. 15	Firma inwestycyjna prowadząca alternatywny system obrotu lub zorganizowaną platformę obrotu informuje Komisję Nadzoru Finansowego o przypadku istotnego naruszenia regulacji dotyczących obrotu dokonywanego w tej firmie inwestycyjnej lub zasad uczciwego obrotu, oraz istotnych zakłóceniach funkcjonowania jej systemu informatycznego.
Art. 15	Art. 81 a	Przewiduje możliwość powierzenia przedsiębiorcy lub przedsiębiorcy zagranicznemu wykonywania procesu, usługi lub działalności, które w innym przypadku zostałyby wykonane przez samą firmę inwestycyjną, w tym możliwość wykonywania całości albo części funkcji operacyjnych dotyczących systemów transakcyjnych pozwalających na stosowanie lub wspierających stosowanie handlu algorytmicznego.
Art. 15	Art. 83a	Obowiązek firm inwestycyjnych do stosowania w prowadzonej działalności rozwiązań technicznych i organizacyjnych zapewniających bezpieczeństwo i ciągłość świadczonych usług maklerskich oraz ochronę interesów klientów i informacji poufnych lub stanowiących tajemnicę zawodową.

8.4 Ustawa z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2022r. poz. 170 z późn. zm.)

Tabela porównawcza

Akt Prawny	**Ustawa z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2022r. poz. 170 z późn. zm.)**	
Art. 15	Art. 4 pkt 2	Celem działania spółki prowadzącej giełdę jest zapewnienie bezpiecznego i sprawnego przebiegu transakcji giełdowych i rozliczeń.

8.5 Rozporządzenie Ministra Finansów z dnia 8 grudnia 2021 r. w sprawie szacowania kapitału wewnętrznego i aktywów płynnych, systemu zarządzania ryzykiem, badania i oceny nadzorczej, a także polityki wynagrodzeń w domu maklerskim oraz małym domu maklerskim.

Tabela porównawcza

Akt Prawny	**Rozporządzenie Ministra Finansów z dnia 8 grudnia 2021 r. w sprawie szacowania kapitału wewnętrznego i aktywów płynnych, systemu zarządzania ryzykiem, badania i oceny nadzorczej, a także polityki wynagrodzeń w domu maklerskim oraz małym domu maklerskim**	
AIA	Rozporządzenie	Opis
Art. 15	§ 6 ust. 3	Obowiązek zapewnienia przez zarząd i radę nadzorczą domu maklerskiego lub małego domu maklerskiego odpowiednich zasobów, w tym informatycznych niezbędnych do należytego zarządzania ryzykiem.

8.6 Rozporządzenie Ministra Finansów z dnia 30 maja 2018 r. w sprawie trybu i warunków postępowania firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy 21 o obrocie instrumentami finansowymi, oraz banków powierniczych (Dz.U. z 2018 r., poz. 1112 z późn. zm.).

Tabela porównawcza

Akt Prawny	**Rozporządzenie Ministra Finansów z dnia 30 maja 2018 r. w sprawie trybu i warunków postępowania firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy 21 o obrocie instrumentami finansowymi, oraz banków powierniczych (Dz.U. z 2018 r., poz. 1112 z późn. zm.)**	
AIA	Rozporządzenie	Opis
Art. 3 pkt 1	§ 1	Rozporządzenie określa tryb i warunki postępowania firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi oraz banków powierniczych w zakresie czynności, do wykonywania, których mogą być stosowane systemy sztucznej inteligencji.

8.7 Rozporządzenie Ministra Finansów z dnia 30 maja 2018 r. w sprawie trybu i warunków postępowania firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy 21 o obrocie instrumentami finansowymi, oraz banków powierniczych (Dz.U. z 2018 r., poz. 1112 z późn. zm.)

Tabela porównawcza

Akt Prawny	**Rozporządzenie Ministra Finansów z dnia 29 maja 2018 r. w sprawie szczegółowych warunków technicznych i organizacyjnych dla firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy 21 o obrocie instrumentami finansowymi, oraz banków powierniczych (Dz.U. z 2018 r., poz. 1111 z późn. zm.)**	
AIA	Rozporządzenie	Opis
Art. 3 pkt 1	§ 1	Rozporządzenie określa szczegółowe warunki techniczne i organizacyjne wymagane do prowadzenia działalności przez firmę inwestycyjną i bank, o którym mowa w art. 70 ust. 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, oraz do prowadzenia rachunku papierów wartościowych, rachunków derywatów i rachunków zbiorczych przez bank powierniczy, które w swojej działalności mogą wykorzystywać systemy sztucznej inteligencji.
Art. 15	§ 21	Rozporządzenie określa szczegółowe warunki techniczne i organizacyjne jakim podlegają systemy informatyczne firm inwestycyjnych i banków, o których mowa w art. 70 ust. 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.

8.8 Rekomendacja D Komisji Nadzoru Finansowego dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach

Tabela porównawcza

Akt Prawny	**Rekomendacja D Komisji Nadzoru Finansowego dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach**	
AIA	Rekomendacja D	Opis
Art. 15	Cała Rekomendacja	Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka. Biorąc pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego banków zagadnienia te powinny być rozpatrywane w połączeniu ze zbiorem dobrych praktyk wskazanych w rekomendacji organu nadzoru banku. Rekomendacja D ma na celu wskazanie bankom oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami.

8.9 Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe

Tabela porównawcza

Akt Prawny	**Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (tj.: Dz.U. z 2022 r., poz. 2324, ze zm.)**	
AIA	Ustawa Prawo bankowe	Opis
Art. 3 pkt 1	Art. 1 pkt 1	Banki, oddziały i przedstawicielstwa banków zagranicznych, a także oddziały instytucji kredytowych mogą wykorzystywać w swojej działalności systemy sztucznej inteligencji.
motyw 37 uzasadn.; Art. 6 ust. 2	Art. 105a ust. 1a	Banki, inne instytucje ustawowo upoważnione do udzielania kredytów, instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, a także instytucje utworzone na podstawie art. 105 ust. 4, mogą w celu oceny zdolności kredytowej i analizy ryzyka kredytowego podejmować decyzje, opierając

		się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, danych osobowych – również stanowiących tajemnicę bankową – pod warunkiem zapewnienia osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz do wyrażenia własnego stanowiska.
Art. 9	Art. 9 ust. 3 w zw. z Art. 9b	W banku funkcjonuje system zarządzania, który stanowi zbiór zasad i mechanizmów odnoszących się do procesów decyzyjnych, zachodzących w banku oraz do oceny prowadzonej działalności bankowej. W ramach systemu zarządzania w banku funkcjonuje system zarządzania ryzykiem. Instytucje kredytowe podlegające przepisom dyrektywy 2013/36/UE muszą posiadać solidne zasady zarządzania obejmujące jasną strukturę organizacyjną z dobrze określonymi, przejrzystymi i spójnymi zakresami odpowiedzialności, skuteczne procedury służące identyfikacji ryzyka, na które te instytucje są lub mogą być narażone, zarządzania tym ryzykiem, monitorowania i zgłaszania go, odpowiednie mechanizmy kontroli wewnętrznej obejmujące należyte procedury administracyjne i księgowe, sieci i systemy informatyczne utworzone i zarządzane zgodnie z rozporządzeniem (UE) 2022/2554 oraz politykę i praktyki wynagrodzeń zgodne z zasadami należytego i skutecznego zarządzania ryzykiem i sprzyjające takiemu zarządzaniu. Zgodnie z art. 9 AIA ustanawia się, wdraża, dokumentuje i utrzymuje system zarządzania ryzykiem w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka, który w przypadku instytucji kredytowych podlegających przepisom dyrektywy 2013/36/UE stanowi część procedur służących zarządzaniu ryzykiem ustanowionych przez te instytucje zgodnie z art. 74 tej dyrektywy.
Art. 17	Art. 9 ust. 3 w zw. z Art. 9b	Dostawcy systemów sztucznej inteligencji wysokiego ryzyka wprowadzają system zarządzania jakością, który zapewnia zgodność z niniejszym rozporządzeniem. Jeżeli chodzi o dostawców będących instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE, obowiązek wprowadzenia systemu zarządzania jakością uznaje się za spełniony w przypadku zapewnienia zgodności z przepisami dotyczącymi zasad, procedur i mechanizmów

		zarządzania wewnętrznego ustanowionymi w art. 74 tej dyrektywy.
Art. 18	Art. 9 ust. 3 w zw. z art. 9b	Dostawcy systemów sztucznej inteligencji wysokiego ryzyka sporządzają dokumentację techniczną, o której mowa w art. 11 AIA, zgodnie z załącznikiem IV AIA, przy czym dostawcy będący instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE prowadzą dokumentację techniczną jako jeden z elementów dokumentacji dotyczącej zasad, procedur i mechanizmów zarządzania wewnętrznego zgodnie z art. 74 tej dyrektywy.
Art. 20	Art. 9 ust. 3 w zw. z art. 9b	Dostawcy systemów sztucznej inteligencji wysokiego ryzyka przechowują rejestry zdarzeń generowane automatycznie przez ich systemy sztucznej inteligencji wysokiego ryzyka, o ile tego rodzaju rejestry znajdują się pod ich kontrolą na podstawie ustaleń umownych z użytkownikiem lub z mocy prawa. Dostawcy będący instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE przechowują rejestry zdarzeń wygenerowane przez ich systemy sztucznej inteligencji wysokiego ryzyka jako jeden z elementów dokumentacji zgodnie z art. 74 tej dyrektywy.
Art. 29 ust. 4	Art. 9 ust. 3 w zw. z art. 9b	Użytkownicy monitorują działanie systemu sztucznej inteligencji wysokiego ryzyka w oparciu o instrukcję obsługi. W odniesieniu do użytkowników będących instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE obowiązek w zakresie monitorowania, o którym mowa w zdaniu pierwszym, uznaje się za spełniony w przypadku zapewnienia zgodności z przepisami dotyczącymi zasad, procedur i mechanizmów zarządzania wewnętrznego ustanowionymi w art. 74 tej dyrektywy.
Art. 29 ust. 5	Art. 9 ust. 3 zw. z art. 9b	Użytkownicy systemów sztucznej inteligencji wysokiego ryzyka przechowują rejestry zdarzeń generowane automatycznie przez dany system sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod ich kontrolą. Rejestry zdarzeń przechowuje się przez okres odpowiedni w świetle przeznaczenia systemu sztucznej inteligencji wysokiego ryzyka i mających zastosowanie zobowiązań prawnych przewidzianych w prawie Unii lub prawie krajowym. Użytkownicy będący instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE przechowują rejestry zdarzeń jako jeden z elementów

		dokumentacji dotyczącej zasad, procedur i mechanizmów zarządzania wewnętrznego zgodnie z art. 74 tej dyrektywy.
Art. 19	Art. 133a	W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b) AIA, wprowadzanych do obrotu lub oddawanych do użytku przez dostawców będących instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE, ocenę zgodności przeprowadza się w toku procedury, o której mowa w art. 97-101 tej dyrektywy. Komisja Nadzoru Finansowego co najmniej raz w roku przeprowadza badanie i ocenę nadzorczą banku albo przegląd i weryfikację wyników poprzedniego badania i oceny nadzorczej.
Art. 43 ust. 2	Art. 133a	W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 2-8 AIA, dostawcy postępują zgodnie z procedurą oceny zgodności opierająca się na kontroli wewnętrznej, o której mowa w załączniku VI i która nie przewiduje udziału jednostki notyfikowanej. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b), wprowadzanych do obrotu lub oddawanych do użytku przez instytucje kredytowe podlegające przepisom dyrektywy 2013/36/UE, ocenę zgodności przeprowadza się w toku procedury, o której mowa w art. 97-101 tej dyrektywy. Komisja Nadzoru Finansowego co najmniej raz w roku przeprowadza badanie i ocenę nadzorczą banku albo przegląd i weryfikację wyników poprzedniego badania i oceny nadzorczej.

8.10 Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych

Tabela porównawcza

Akt Prawny	**Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych**	
AIA	Wytyczne	Opis
Art. 15	Całe wytyczne	Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka.

		Biorąc pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego powszechnych towarzystw emerytalnych zagadnienia te powinny być rozpatrywane w połączeniu ze zbiorem dobrych praktyk wskazanych w wytycznych organu nadzoru powszechnych towarzystw emerytalnych. Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych mają na celu wskazanie podmiotom nadzorowanym oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami.

8.11 Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji

Tabela porównawcza

Akt Prawny	Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji	
AIA	Wytyczne	Opis
Art. 15	Całe wytyczne	Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka. Biorąc pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji zagadnienia te powinny być rozpatrywane w połączeniu ze zbiorem dobrych praktyk wskazanych w wytycznych organu nadzoru zakładów ubezpieczeń i zakładów reasekuracji. Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji mają na celu wskazanie podmiotom nadzorowanym oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami.

8.12 Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych

Tabela porównawcza

Akt Prawny	**Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych**	
AIA	Wytyczne	Opis
Art. 15	Całe wytyczne	Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka. Biorąc pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych zagadnienia te powinny być rozpatrywane w połączeniu ze zbiorem dobrych praktyk wskazanych w wytycznych organu nadzoru towarzystwach funduszy inwestycyjnych. Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych mają na celu wskazanie podmiotom nadzorowanym oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami.

8.13 Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych

Tabela porównawcza

Akt Prawny	**Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych**	
AIA	Wytyczne	Opis
Art. 15	Całe wytyczne	Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka. Biorąc pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego w firmach inwestycyjnych zagadnienia te powinny być rozpatrywane w połączeniu ze zbiorem dobrych praktyk wskazanych w wytycznych organu nadzoru firm inwestycyjnych. Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych mają na celu wskazanie podmiotom nadzorowanym oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami.

8.14 Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych

Tabela porównawcza

Akt Prawny	**Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych**	
AIA	Rekomendacja D-SKOK	Opis
Art. 15	Cała rekomendacja	Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka. Biorąc pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych zagadnienia te powinny być rozpatrywane w połączeniu ze zbiorem dobrych praktyk wskazanych w wytycznych organu nadzoru firm inwestycyjnych. Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych ma na celu wskazanie podmiotom nadzorowanym oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami.

8.15 Rekomendacja W dotycząca zarządzania ryzykiem modeli w bankach

Tabela porównawcza

Akt Prawny	Rekomendacja W dotycząca zarządzania ryzykiem modeli w bankach	
AIA	Rekomendacja W	Opis
Art. 15	Cała rekomendacja	Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka. Biorąc pod uwagę zwiększenie zakresu wykorzystania modeli rozumianych jako, narzędzi służących do sporządzania ograniczonych (do najistotniejszych wymiarów) opisów wybranego aspektu rzeczywistości, zagadnienia z nimi związane powinny być rozpatrywane w połączeniu ze zbiorem dobrych praktyk wskazanych w wytycznych organu nadzoru firm inwestycyjnych. Rekomendacja W określa m.in. standardy procesu zarządzania ryzykiem modeli, z uwzględnieniem potrzeby określenia ram dla tego procesu, w tym zasad budowy modeli oraz oceny jakości ich działania, przy zapewnieniu właściwych rozwiązań w ramach ładu korporacyjnego

8.16 Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej

Tabela porównawcza

Akt Prawny	Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej	
AIA	Komunikat Chmurowy	Opis
Art. 15	Cały komunikat	Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka. Przetwarzanie informacji prawnie chronionych w chmurze obliczeniowej generuje ryzyka związane z ochroną przetwarzanych informacji. Ochrona przetwarzania informacji istotnych dla procesów lub działania podmiotu nadzorowanego przez UKNF wymaga wzięcia pod uwagę zagadnień wskazanych w Komunikacie Chmurowym

9. Prawo konsumenckie

9.1 Wstęp

Wpływ projektowanego AIA na konsumentów jest oczywisty, ponieważ są oni końcowymi odbiorcami zastosowań systemów sztucznej inteligencji. Mimo tego, nawiązania do prawa konsumenckiego i konsumentów wprawdzie pojawiają się w uzasadnieniu projektu i w AIA, lecz tylko w kilku miejscach.

W uzasadnieniu AIA wskazano, że:

- wybór formy rozporządzenia i przyjęte rozwiązania, zwłaszcza te dotyczące systemów wysokiego ryzyka, zapewnią pewność prawa zarówno podmiotom gospodarczym, jak i konsumentom (pkt 2.4);
- przyszłe rozporządzenie wzmocni i będzie promować ochronę praw chronionych Kartą praw podstawowych Unii Europejskiej, do których należy wysoki poziom ochrony konsumentów regulowany przez jej art. 38 (pkt 3.5 oraz motyw 28);
- wprowadzone ograniczenia wolności prowadzenia działalności gospodarczej mają zapewnić zgodność z nadrzędnym interesem publicznym, przejawiającym się m.in. w ochronie konsumentów (pkt 3.5);
- projekt jest spójny z prawem wtórnym Unii dotyczącym ochrony konsumentów (pkt 1.2).

W samym AIA konsument nie pojawia się w jego części normatywnej, lecz tylko raz we wskazanym wyżej motywie 28. Motyw 28 przedstawia prawa konsumentów w kontekście praw podstawowych, bowiem zgodnie z nim: „(...) Przy klasyfikowaniu systemu sztucznej inteligencji jako systemu wysokiego ryzyka zasadnicze znaczenie ma skala szkodliwego wpływu wywieranego przez system sztucznej inteligencji na prawa podstawowe chronione na mocy Karty. Do praw tych należą: prawo do godności człowieka, poszanowanie życia prywatnego i rodzinnego, ochrona danych osobowych, wolność wypowiedzi i informacji, wolność zgromadzania się i stowarzyszania się oraz niedyskryminacja, **ochrona konsumentów**, prawa pracownicze, prawa osób niepełnosprawnych, prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawo do obrony i domniemania niewinności, prawo do dobrej administracji (...)".

Brak odwołań do konsumentów w AIA wynika z tego, że niewiele przepisów dotyczy bezpośrednio konsumentów. Nie umniejsza to jednak ani znaczenia AIA dla konsumentów, ani nie oznacza braku konieczności określenia związku wielu przepisów z prawem konsumenckim.

Ze względu na rozległy charakter tej dziedziny prawa, poniżej zostaną przedstawione najważniejsze akty prawa konsumenckiego: 1) dyrektywa 2005/29/WE o nieuczciwych praktykach handlowych i jej implementacja do prawa polskiego w postaci ustawy z 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym oraz 2) dyrektywa 2011/83/UE w sprawie praw konsumentów wraz z ustawą z dnia 30 maja 2014 r. o prawach konsumenta.

9.2 Dyrektywa 2005/29/WE o nieuczciwych praktykach handlowych/ Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym

Przepisy AIA wykazują duże podobieństwo do niektórych przepisów dyrektywy 2005/29/WE i, odpowiednio, przepisów polskiej ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym. Choć mają niekiedy szerszy zakres podmiotowy, obejmując nie tylko relacje przedsiębiorca – konsument, mogą być w zakresie relacji B2C porównywane do typowych przepisów wskazanych wyżej aktów prawnych. Ich interpretacja zatem może być ułatwiona, lecz nie powinna być kalką ze względu na odrębności niektórych przesłanek.

Tabela porównawcza

Akt Prawny	**Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. o nieuczciwych praktykach handlowych (UCPD)/ Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym**	
AIA	**UCPD/u.p.n.p.r.**	**Opis**
Tytuł II (Art. 5)	Art. 2 lit. d UCPD/ Art. 2 lit. pkt 4 u.p.n.p.r. załącznik I do UCPD/ art. 7 i 9 u.p.n.p.r.	Tytuł II AIA składa się wyłącznie z art. 5 i wprowadza zakaz określonych praktyk w zakresie sztucznej inteligencji. AIA posługuje się zatem terminem „praktyka”, podczas gdy dyrektywa 2005/29/WE pojęciem „praktyka handlowa”, a ustawa polska implementująca dyrektywę – pojęciem „praktyka rynkowa”. W wielu przypadkach pojęcie „praktyka” będzie tożsame z pojęciem „praktyka handlowa/rynkowa”, ponieważ niektóre praktyki wymienione w art. 5 mogą dotyczyć relacji przedsiębiorca-konsument oraz mieć charakter komercyjny, odpowiadający definicji z art. 2 lit. d dyrektywy 2005/29/WE/ art. 2 pkt 4 u.p.n.p.r. Zakazy praktyk w zakresie sztucznej inteligencji z art. 5 AIA przypominają zakazy praktyk handlowych w każdych okolicznościach z załącznika I do dyrektywy 2005/29/WE / art. 7 i 9 u.p.n.p.r. Nie ograniczają się jednak do naruszeń interesów gospodarczych konsumentów, lecz uwzględniają wyrządzenie szkody fizycznej lub psychicznej danych osób. Można zatem stwierdzić, że zakazy z art. 5, co najmniej w pewnym zakresie, np. w przypadku stosowania technik podprogowych (art. 5 ust. 1 lit. a), wykorzystywania słabości określonej grupy osób (art. 5 ust. 1 lit. b) mogą być uznawane za zakazy per se nieuczciwych praktyk handlowych.
Art. 52 ust. 2 i 3	Art. 2 lit. d UCPD / Art. 2 lit. pkt 4 u.p.n.p.r.	Artykuł 52 ust. 2 i 3 AIA dotyczy relacji między użytkownikami systemów sztucznej inteligencji a osobami fizycznymi, będącymi odbiorcami określonych systemów sztucznej inteligencji lub

	Art. 7 UCPD/ Art. 6 u.p.n.p.r. Art. 8 UCPD/ Art. 8 u.p.n.p.r. załącznik II do UCPD	podmiotami, wobec których się je stosuje. W wielu sytuacjach osoby te będą konsumentami. Wówczas analizowane przepisy są bliskie dyrektywie 2005/29/WE/ ustawie o przeciwdziałaniu nieuczciwym praktykom rynkowym. Również zakres przedmiotowy jest zbliżony, bowiem wielokrotnie stosowanie systemów rozpoznawania emocji lub systemów kategoryzacji biometrycznej (art. 52 ust. 2) oraz stosowanie deepfake'ów (art. 52 ust. 3) może być elementem praktyki handlowej/rynkowej w rozumieniu, odpowiednio, art. 2 lit. d dyrektywy 2005/29/WE / art. 2 lit. pkt 4 u.p.n.p.r. Zarówno art. 52 ust. 2, jak i art. 52 ust. 3 AIA wprowadzają typowy obowiązek informacyjny polegający na informowaniu osób fizycznych, które mogą być konsumentami, o stosowaniu wobec nich określonych systemów sztucznej inteligencji. Nieprzekazanie tych informacji konsumentom może być ocenione jako zaniechanie wprowadzające w błąd na podstawie art. 7 dyrektywy 2005/29/WE / art. 6 u.p.n.p.r. W związku z tymi projektowanymi przepisami zmianie powinien ulec załącznik II do dyrektywy 2005/29/WE, który zawiera wymogi informacyjne ustanowione w prawie unijnym, dotyczące komunikacji handlowej, w tym reklamy i marketingu, stanowiące istotną informację w rozumieniu art. 7 ust. 4 dyrektywy 2005/29/WE. Załącznik ten ma wprawdzie niewyczerpujący charakter, lecz nie był aktualizowany od uchwalenia dyrektywy o nieuczciwych praktykach handlowych w 2005 r. Osłabia to znacznie jego informacyjny charakter. Nieprzekazanie konsumentowi informacji wymaganych art. 52 ust. 2 i 3 AIA lub przekazanie ich w sposób niejasny lub nieadekwatny może być oceniane jako agresywna praktyka handlowa (art. 8 dyrektywy 2005/29/WE / art. 8 u.p.n.p.r.). Choć AIA nie reguluje relacji między nim a dyrektywą 2005/29/WE nie ma przeszkód, by akty te stosować równolegle, jeżeli praktyka handlowa dotyczy relacji między przedsiębiorcą a konsumentem. Odpowiednio stosować można ustawę o przeciwdziałaniu nieuczciwym praktykom rynkowym razem z AIA.

9.3 Dyrektywa 2011/83/UE w sprawie praw konsumentów/ Ustawa z 30 maja 2014 r. o prawach konsumenta

Mapowanie dyrektywy 2011/83/UE i ustawy o prawach konsumenta w świetle AIA wymaga podkreślenia, że ich zakres podmiotowy jest odmienny niż wskazanych przepisów AIA. W szczególności art. 13 i 14 AIA nie znajdzie zastosowania do relacji przedsiębiorca - konsument. Niemniej jednak warto wskazać zwłaszcza na przepisy dotyczące obowiązków informacyjnych w dyrektywie 2011/83/UE i, odpowiednio, ustawy o prawach konsumenta, ponieważ może to stanowić punkt wyjścia dla refleksji o konieczności wprowadzenia odpowiednich zasad dla relacji B2C.

Tabela porównawcza

Akt Prawny	Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25.10.2011 r. w sprawie praw konsumentów (CRD)/ Ustawa z dnia 30 maja 2014 r. o prawach konsumenta	
AIA	CRD/u.p.k.	Opis
Art. 13	zwłaszcza art. 6 CRD / Art. 12 u.p.k.	Należy zwrócić uwagę na rozdział II AIA, a zwłaszcza art. 13, który wprowadza wymogi dotyczące przejrzystości odnoszące się do systemów sztucznej inteligencji wysokiego ryzyka oraz podobieństwo art. 12 u.p.k. pod kątem informacji przekazywanych konsumentom. Jednak zgodnie z art. 13 AIA, dostawca musi zapewnić przejrzystość tylko w stosunku do użytkownika systemu, a nie do konsumenta. Dlatego można się zastanawiać, w jakim zakresie należałoby zapewnić przejrzystość zastosowania SI wobec konsumenta i czy nie powinno to być narzucone przez AIA. Istotne byłoby, żeby w procesie zawierania umowy z konsumentem lub w toku działań zmierzających do zawarcia takiej umowy konieczne jest informowanie konsumenta o wykorzystywaniu systemu SI wysokiego ryzyka wraz ze wskazaniem możliwych sposobów oddziaływania takiego systemu na konsumenta oraz zagrożeń wywoływanych przez ten system dla konsumenta. Przy aktualnej treści załącznika III AIA nie byłoby to stosowane szeroko do konsumentów, jednak w obszarze identyfikacji i kategoryzacji biometrycznej już tak. Zapewniłoby to kompleksową przejrzystość systemu. Nie tylko w relacji do użytkownika, jak to wynika z AIA, lecz także wobec konsumentów. Artykuł 13 AIA nie określa zobowiązania do zapewnienia przejrzystości osobie, której dotyczy prognoza lub decyzja oparta na sztucznej inteligencji, co czyni np. art. 6 ust. 1 lit. ea CRD, zgodnie z którym zanim

		konsument zostanie związany umową zawieraną na odległość lub umową zawieraną poza lokalem przedsiębiorstwa, lub jakąkolwiek ofertą w tym zakresie, przedsiębiorca jest zobowiązany w jasny i zrozumiały sposób udzielić konsumentowi informacji o tym, że cena została indywidualnie dostosowana w oparciu o zautomatyzowane podejmowanie decyzji (w przypadku, gdy ma to zastosowanie), tak aby mógł on uwzględnić potencjalne ryzyko przy podejmowaniu decyzji o zakupie. Obowiązek ten został ograniczony do sytuacji, gdy personalizacja dokonywana jest za pomocą zautomatyzowanego podejmowania decyzji, przy czym nie obejmuje on tzw. cen dynamicznych. Do rozważenia jest wprowadzenie obowiązku informowania konsumentów o zastosowaniu mechanizmów SI w celu dopasowywania do konsumenta komunikatów marketingowych wraz z podaniem przy komunikacie przyczyn, które zadecydowały o wyświetleniu im takiego przekazu. Zbliżony obowiązek pojawia się w Digital Services Act[9] w odniesieniu do platform internetowych. Jednak dla zapewnienia transparentności procesu decyzyjnego u konsumentów rozsądnym rozwiązaniem byłoby danie im możliwości zrozumienia, dlaczego SI dopasowała do danej osoby określony komunikat marketingowy.
Art. 52 ust. 2 i 3	zwłaszcza Art. 6 CRD/ Art. 12 u.p.k.	Art. 52 ust. 2 i 3 wprowadzają obowiązek informowania i zachowania przejrzystości w odniesieniu do wirtualnych agentów, systemów deepfake i systemów rozpoznawania emocji lub systemów kategoryzacji biometrycznej. Przepisy te ustanawiają zatem typowy obowiązek informacyjny polegający na informowaniu osób fizycznych, które mogą być konsumentami, o stosowaniu wobec nich określonych systemów sztucznej inteligencji. Do rozważenia jest wprowadzenie analogicznych przepisów w dyrektywie 2011/83/UE oraz w ustawie o prawach konsumenta.

[9] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_pl

Ministerstwo
Cyfryzacji

GRAI
GRUPA ROBOCZA
DS. SZTUCZNEJ INTELIGENCJI