

Implementacja Aktu o Sztucznej Inteligencji w polskim sektorze przetwórstwa spożywczego.

Analiza prawna zjawiska Shadow AI



Analiza obecnej sytuacji wskazuje, że polski przemysł spożywczy znajduje się w krytycznej fazie przejściowej, w której brak przygotowania do realizacji rygorów AI Act może skutkować drastycznymi sankcjami finansowymi. Chociaż Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689, znane jako Akt o Sztucznej Inteligencji (AI Act) weszło w życie 1 sierpnia 2024 r., w powszechnej świadomości przedsiębiorców w Polsce dominuje przekonanie o braku realnych zmian w obszarze AI.

Dynamika wdrażania AI Act. Dlaczego rynek nie dostrzega zmian

Powszechne wrażenie, że „nic się nie zmieniło”, jest wynikiem mechanizmu stopniowego stosowania rozporządzenia. Ustawodawca unijny przyjął strategię, w której najbardziej niebezpieczne praktyki są eliminowane natychmiast, podczas gdy wymogi dla systemów wspomagających produkcję czy logistykę są wprowadzane powoli.

Poniższe punkty pokazują etapy wdrażania przepisów, które bezpośrednio wpływają na funkcjonowanie przedsiębiorstw spożywczych w Polsce.

1 sierpnia 2024	Wejście w życie rozporządzenia	Formalny start procesów dostosowawczych w UE
2 lutego 2025	Zakaz praktyk o nieakceptowalnym ryzyku	Konieczność wycofania systemów manipulacyjnych i biometrycznych
2 lutego 2025	Obowiązek budowania kompetencji (AI Literacy)	Wymóg szkolenia pracowników z bezpiecznego korzystania z AI
2 sierpnia 2025	Zarządzanie modelami GPAI (ogólnego przeznaczenia)	Nowe standardy dla dostawców narzędzi typu ChatGPT
2 sierpnia 2025	Powołanie organów nadzoru i systemu kar	Gotowość państw do nakładania sankcji administracyjnych
2 sierpnia 2026	Pełna stosowalność systemów wysokiego ryzyka (załącznik III)	Obowiązek dokumentacji i audytów dla AI w HR i logistyce
2 sierpnia 2027	Systemy AI jako elementy produktów regulowanych	Certyfikacja maszyn produkcyjnych z wbudowaną sztuczną inteligencją

Certyfikacja maszyn produkcyjnych z wbudowaną sztuczną inteligencją

Pełna stosowalność przepisów dla systemów sprzedażowych następuje teraz, w 2026 r., ale od lutego 2025 r. firmy są zobowiązane do zapewnienia pracownikom odpowiedniego poziomu wiedzy o AI (art. 4). Ignorowanie tego zapisu może zostać zweryfikowane podczas kontroli Inspekcji Pracy lub nowo powstającej Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI). To organ doradczy lub parlamentarny zajmujący się wspieraniem rozwoju AI oraz nadzorem

nad jej bezpiecznym wdrażaniem. Analizuje ryzyka technologiczne, społeczne i prawne związane z wykorzystaniem systemów sztucznej inteligencji. Opracowuje rekomendacje regulacyjne, m.in. w kontekście wdrażania przepisów takich jak AI Act. Spokojnie, ta komisja znajduje się dopiero w fazie koncepcji ustawodawczej i jest to planowany organ, który ma powstać w przyszłości – jeszcze nie istnieje formalnie ani nie prowadzi kontroli w praktyce. To nie znaczy, że artykuł ten można odłożyć na potem. Historia pokazała, że organy takie mogą pojawić się bardzo szybko i w realny sposób zagrozić naszemu dobremu samopoczuciu.

Architektura ryzyka w przemyśle spożywczym

Przemysł spożywczy w Polsce, charakteryzujący się wysokim stopniem automatyzacji i skomplikowanymi łańcuchami dostaw, jest naturalnym polem do implementacji systemów AI. AI Act dzieli te systemy na cztery kategorie ryzyka, z których każda niesie inne konsekwencje dla producenta żywności.

Zgodnie z art. 6 i załącznikiem III, systemy AI stają się „wysokim ryzykiem”, gdy wpływają na bezpieczeństwo fizyczne, infrastrukturę krytyczną lub prawa pracowników. W polskim zakładzie produkcyjnym za niezgodne z aktem AI mogą zostać uznane:

1. **Systemy rekrutacyjne i zarządzania personelem.** Automatyczne filtrowanie podań o pracę, systemy oceny wydajności pracowników na liniach rozbioru mięsa lub algorytmy monitorujące zachowania pracowników w celu przydzielania premii.
2. **Infrastruktura krytyczna i logistyka.** AI zarządzające ruchem w magazynach wysokiego składowania (systemy AGV) lub optymalizujące łańcuch chłodniczy, gdzie błąd algorytmu może prowadzić do masowego zepsucia żywności i zagrożenia zdrowia publicznego.
3. **Elementy bezpieczeństwa maszyn.** Inteligentne sensory w maszynach pakujących lub tnących, które mają za zadanie wykrywać obecność człowieka i zatrzymywać proces w sytuacjach awaryjnych.

Takie systemy muszą liczyć się z koniecznością prowadzenia szczegółowej dokumentacji technicznej, rejestrowania logów systemowych przez określony czas oraz zapewnienia stałego nadzoru ludzkiego nad wynikami działania algorytmu.

Shadow AI. Ukryta rewolucja i jej niebezpieczeństwa

Pojęcie Shadow AI odnosi się do zjawiska wykorzystywania przez pracowników narzędzi sztucznej inteligencji bez formalnej zgody, wiedzy i nadzoru działu IT. Jest to bezpośrednia ewolucja znanego od lat Shadow IT, jednak niosąca znacznie większe ryzyko dla integralności danych i zgodności prawnej.

W polskim przemyśle spożywczym presja na optymalizację kosztów i czasu pracy sprawia, że pracownicy biurowi oraz technolodzy sięgają po ogólnodostępne modele językowe takie jak ChatGPT, Claude czy Gemini oraz proste generatory obrazów, traktując je jako darmowe, prywatne narzędzia poprawiające produktywność pracy.

Mechanizmy powstawania Shadow AI

Zjawisko to napędzane jest przez trzy główne czynniki:

1. **Łatwość dostępu.** Większość potężnych narzędzi AI jest dostępna z poziomu przeglądarki w smartfonie, co czyni blokady na komputerach służbowych nieskutecznymi.
2. **Brak oficjalnych narzędzi.** Gdy firma zwleka z wdrożeniem bezpiecznych, korporacyjnych wersji AI, pracownicy sami szukają rozwiązań, aby sprostać rosnącej presji ze strony kierownictwa.
3. **Niska świadomość ryzyka.** Pracownicy często nie rozumieją, że wpisując dane do okna czatu, „karmią” model publiczny danymi, które mogą stać się dostępne dla konkurencji.

Shadow AI w praktyce. Przykłady z przemysłu spożywczego i biura

Aby w pełni zrozumieć zagrożenie, należy przeanalizować konkretne sytuacje w firmie spożywczej, sytuacje z życia biurowego.

Technolog wkleja do publicznego chatbota pełny skład chemiczny autorskiej mieszanki przypraw, prosząc o znalezienie tańszego zamiennika jednego z konserwantów, który nie zmieni pH produktu. Tym samym unikalna receptura, stanowiąca tajemnicę przedsiębiorstwa, trafia na serwery zewnętrznego dostawcy.

Analitik finansowy kopiuje dane z arkusza rachunku zysków i strat (P&L) konkretnej linii produktowej do darmowego narzędzia AI, prosząc o stworzenie prognozy rentowności na kolejny kwartał. Poufne dane o marżach stają się częścią zbioru treningowego.

Kolejny pracownik, tym razem prawnik, używa AI do streszczenia umowy z kluczowym dostawcą surowców. Wgrywa skan umowy zawierający kary umowne, wolumeny dostaw i dane osobowe przedstawicieli stron, naruszając NDA oraz RODO.

Manager planowania produkcji korzysta z nieautoryzowanej wtyczki AI do Excela, która pobiera dane o historycznej



sprzedaży świeżych owoców morza i łączy je z prognozą pogody. Wtyczka ma uprawnienia do odczytu całego dysku sieciowego, co tworzy lukę bezpieczeństwa dla hakerów.

Asystentka zarządu używa AI do transkrypcji nagrania z poufnego spotkania dotyczącego planowanej fuzji z mniejszym przetwórcą. Nagranie jest przetwarzane w chmurze na serwerze o nieznanym poziomie zabezpieczeń.

Programista utrzymujący system ERP w zakładzie używa AI do naprawy błędu w kodzie odpowiedzialnym za śledzenie partii towaru (*traceability*). Wkleja fragmenty kodu źródłowego do bota, ryzykując ujawnienie luk w zabezpieczeniach systemowych.

Inspektor jakości używa AI do wygenerowania raportu z audytu higienicznego. AI „halucynuje”, zamieniając informację o wykryciu *Listerii* w jednej z próbek na stwierdzenie o „marginalnym zanieczyszczeniu środowiskowym”, co usypia czujność zarządu i prowadzi do wypuszczenia niebezpiecznej partii towaru.

Koordinator BHP prosi AI o przygotowanie instrukcji bezpiecznej pracy przy nowym autoklawie. AI tworzy instrukcję, która brzmi profesjonalnie, ale podaje błędne ciśnienie krytyczne dla tego modelu urządzenia, co stwarza ryzyko wybuchu.

Te dwa ostatnie przykłady niosą za sobą konsekwencje z zakresu prawa karnego i w sposób bezpośredni grożą karami więzienia. Tłumaczenie pomyłkami AI w tym momencie jeszcze pogarsza położenie oskarżonych.

Dział marketingu używa AI do generowania zdjęć produktów (np. soczystych owoców na opakowaniu soku), które nie

odzwierciedlają rzeczywistego składu. Brak oznaczenia „obraz wygenerowany przez AI” narusza wymogi przejrzystości AI Act i może zostać uznany za wprowadzanie konsumenta w błąd.

Konsekwencje braku nadzoru. Scenariusz kontroli KRiBSI

Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji nie ma. Planowany termin przyjęcia projektu przez RM to I kwartał 2026 r. Brak jednak informacji o terminie realizacji tego projektu¹. Więc mamy czas.

Wiele polskich firm spożywczych opiera swoją strategię na dawaniu luzu pracownikom w nadziei na wzrost innowacyjności. Jednak AI Act przewiduje surowe mechanizmy weryfikacji, które zaczną być kiedyś egzekwowane.

Zgodnie z polskimi projektami ustaw, KRiBSI będzie niezależnym organem z szerokimi uprawnieniami kontrolnymi. Procedura kontrolna może wyglądać następująco.

- **Audyt systemowy.** Inspektorzy mogą zażądać dostępu do kodów źródłowych, logów i dokumentacji technicznej każdego systemu AI uznanego za wysokie ryzyko.
- **Weryfikacja kompetencji.** Kontrola może sprawdzić, czy firma wywiązała się z obowiązku AI Literacy, tzn. czy pracownicy wiedzą, jakich narzędzi mogą używać i jakie są limity tej technologii.
- **Badanie Shadow AI.** Wykorzystanie narzędzi do monitorowania ruchu sieciowego może ujawnić, że pracownicy przesyłają dane firmowe do niezatwierdzonych modeli publicznych, co zostanie zakwalifikowane jako brak odpowiedniego systemu zarządzania ryzykiem.

Sankcje finansowe i operacyjne

Brak przygotowania do kontroli może skutkować nałożeniem kar administracyjnych, które w przypadku dużych przedsiębiorstw są naliczane jako procent rocznego obrotu.

Rodzaj przewinienia	Maksymalna kara (EUR)	Maksymalna kara (% obrotu)
Stosowanie praktyk zakazanych (np. manipulacja)	35 000 000	7%
Nieprzestrzeganie wymogów dla AI wysokiego ryzyka	15 000 000	3%
Podawanie niepełnych lub błędnych informacji organom	7 500 000	1%

Oprócz kar finansowych, organ nadzoru ma prawo nakazać natychmiastowe wycofanie systemu AI z rynku lub zaprzestanie jego użytkowania, co w przypadku AI zintegrowanego z linią produkcyjną może oznaczać zatrzymanie zakładu na wiele dni.

Mit bezpieczeństwa wielkich korporacji

Wielkie firmy z sektora spożywczego w Polsce często wykazują postawę, którą można nazwać „bezpieczeństwem w ignorancji”. Opiera się ona na błędnym założeniu, że duża

skala działalności, działy prawne i dotychczasowy brak kar za AI chronią je przed ryzykiem. Rzeczywistość jest jednak inna.

Rozproszona odpowiedzialność. W dużych strukturach łatwiej o powstanie silosów Shadow AI. Gdy dział marketingu „bawi się” w AI, zarząd może być przekonany, że firma jest bezpieczna, podczas gdy ryzyko prawne już rośnie.

Odpowiedzialność za dostawców. Giganci często kupują gotowe rozwiązania od startupów. AI Act nakłada na podmiot stosujący (dużą firmę) obowiązek sprawdzenia czy dostawca spełnił wymogi rozporządzenia. Kupno „czarnej skrzynki” bez certyfikatu CE jest bezpośrednim narażeniem się na karę. Wiadac tu, że komisja z własnej wyгоды może sprawdzać certyfikaty bardziej niż zadawać sobie trud grzebania w algorytmach kodu.

Pułapka PoC (Proof of Concept). Wiele firm testuje AI w ramach pilotaży. AI Act nie zwalnia z obowiązków systemów w fazie testów, jeśli mają one wpływ na rzeczywiste procesy lub dane osób fizycznych. Nie wiadomo czy weryfikacja nie będzie dotyczyć projektów w fazie „papierowych rozważań”.

Dla spółek giełdowych kara za AI Act to nie tylko koszt, ale potężny cios w ratingi ESG i zaufanie inwestorów. Informacja o „nieetycznej sztucznej inteligencji” w produkcji żywności może wywołać bojkot konsumencki.

Wielkie firmy są bardziej widoczne dla regulatorów. KRiBSI, chcąc ustanowić standardy na rynku, w pierwszej kolejności skieruje swoje kroki do liderów branży, traktując ich jako przykład dla całego sektora. Nie trudno zauważyć, że na pierwszy ogień pójść znane, bogate marki. Nie obejdzie się bez spektakularnych przykładowych kar. Każdy urząd (szczególnie



¹ <https://www.gov.pl/web/premier/projekt-ustawy-o-systemach-sztucznej-inteligencji>

nowy) musi wyrobić sobie „szacunek”. Warto przypomnieć, że kiedy wprowadzono RODO czy Inspekcję Transportu Drogowego (ITD) informacje o gigantycznych, przykładowych karach wstrząsały rynkiem

Zarządzanie zgodnością. Jak przetrwać audyt AI Act

Przygotowanie do wejścia w życie pełnych rygorów w 2026 r. wymaga od firm spożywczych podjęcia systematycznych działań. Zgodność z AI Act nie jest jednorazowym wydarzeniem, lecz procesem ciągłym. Proces ten na pewno będzie trwał kilkanaście miesięcy. Czy na pewno mamy tyle czasu?

Elementy systemu zarządzania AI

Firmy powinny wdrożyć model oparty na następujących filarach:

- **Centralny rejestr systemów AI.** Dokumentacja każdego używanego narzędzia, jego przeznaczenia, źródła danych i klasyfikacji ryzyka.
- **Analiza FRIA** (*Fundamental Rights Impact Assessment*). Obowiązkowa dla systemów wysokiego ryzyka. Musi oceniać, jak AI wpływa na prywatność, niedyskryminację i bezpieczeństwo pracowników.
- **Procedury nadzoru ludzkiego.** Wyznaczenie konkretnych osób odpowiedzialnych za weryfikację wyników AI oraz zapewnienie im narzędzi do „wyłączenia” systemu w razie awarii.
- **Zasady czyszczenia danych.** Upewnienie się, że dane treningowe są reprezentatywne i wolne od błędów, co w przemyśle spożywczym oznacza np. uwzględnienie zmienności surowca w różnych porach roku.

Kluczowe wnioski dla kadry zarządzającej

AI Literacy to priorytet na dziś. Obowiązek szkoleniowy wynikający z art. 4 jest najłatwiejszym punktem do zweryfikowania przez inspektorów. Pamiętajmy – szkolenia są relatywnie tanią metodą na zbudowanie pierwszej skutecznej linii obrony.

Shadow AI to realne zagrożenie prawne. Wykorzystywanie darmowych narzędzi przez pracowników bez kontroli to prosta droga do wycieku tajemnic handlowych i naruszenia AI Act.

Zacząłbym od tego, aby wprowadzić „na papierze” zakaz korzystania z narzędzi AI w pracy. Będzie to trudny do zbiccia argument przy każdej kontroli.

Ignorancja jest kosztowna. Wielkie firmy spożywcze, ze względu na swoją ekspozycję rynkową, będą pierwszymi obiektami kontroli KRIBSI. Brak certyfikacji systemów wbudowanych w linie produkcyjne po 2027 r. uniemożliwi sprzedaż produktów na rynku UE. Tutaj liczyłbym na współpracę z dostawcami rozwiązań. Oni również muszą pamiętać o tych certyfikatach. Bez tego nie sprzedadzą swoich urządzeń.

Etyka i przejrzystość budują wartość. Znakowanie treści generowanych przez AI oraz zapewnienie, że algorytmy nie



dyskryminują pracowników, stanie się elementem przewagi konkurencyjnej w relacjach z sieciami handlowymi. To również jest dość proste do realizacji. Jeśli firma jasno oznacza, które opisy produktów, grafiki, rekomendacje są generowane przez AI, to pokazuje, że działa transparentnie, że nie manipuluje odbiorcą zgodna z regulacjami AI Act.

Przedsiębiorstwa powinny niezwłocznie przejść od modelu przypadkowych eksperymentów z AI do modelu uporządkowanego zarządzania ryzykiem AI Governance. Tylko takie podejście pozwoli na bezpieczne wykorzystanie potencjału sztucznej inteligencji w optymalizacji produkcji żywności, przy jednoczesnym uniknięciu kar, które mogą zagrozić dalszemu istnieniu organizacji.

Oczekiwanie na „pierwsze kary u konkurencji” może okazać się spóźnioną strategią, gdyż system sankcji w AI Act jest zaprojektowany tak, aby dotkliwie karać za wieloletnie zaniedbania w budowaniu struktur nadzoru. Czy mamy jeszcze czas na przyglądanie się zjawisku?

Wojciech Moszczyński

Wojciech Moszczyński – absolwent Katedry Ekonometrii i Statystyki Uniwersytetu Mikołaja Kopernika w Toruniu; specjalista z zakresu ekonometrii, finansów, data science oraz rachunkowości zarządczej. Specjalizuje się w optymalizacji procesów produkcyjnych i logistycznych. Prowadzi badania w obszarze rozwoju i zastosowania sztucznej inteligencji. Od lat zaangażowany w popularyzację machine learning oraz data science w środowiskach biznesowych.