t. LXXVI • nr 11/2023 (905) • DOI 10.33226/0137-5490.2023.11.3

Dr Gabriela Bar

Uniwersytet Śląski w Katowicach
ORCID 0000-0002-0924-2693
e-mail: gabriela.bar@szostek-bar.pl

Dr Rafał Skibicki

Uniwersytet Śląski w Katowicach
ORCID 0000-0003-1194-4173
e-mail: rafal.skibicki@szostek-bar.pl

Dane w inteligentnej fabryce – aspekty prawne[1]

Data in a smart factory – legal aspects

Streszczenie

W dobie Przemysłu 4.0 wykorzystuje się coraz częściej usługi chmurowe oferujące integrację różnorodnych systemów informatycznych oraz systemy sztucznej inteligencji (AI), wspierające elastyczność procesów oraz modularyzację. Tworzone są platformy umożliwiające synchronizację działania różnych agentów AI oraz opracowywane są komponenty przemysłowe oparte na AI, zintegrowane w systemach wieloagentowych. Jednym z istotnych aspektów inteligentnej produkcji jest bezpieczna i efektywna współpraca człowieka z robotami przemysłowymi i systemami AI. W tym kontekście autorzy niniejszego artykułu rozważają kwestie dotyczące rodzaju i zakresu przetwarzanych danych, przetwarzania mieszanych zbiorów danych oraz zjawiska ponownej personalizacji danych, zakresu prawa do prywatności oraz zautomatyzowanego podejmowania decyzji i ich wyjaśnialności. Wskazują też na nowe lub projektowane regulacje prawne, które mogą mieć wpływ na inteligentną produkcję.

Słowa kluczowe: inteligentna produkcja, Przemysł 4.0, sztuczna inteligencja, dane, zarządzanie danymi

JEL: K11, K12, K24

Abstract

In the era of Industry 4.0, cloud services have become commonly used, offering integration of various IT systems. Artificial Intelligence (AI) systems support process flexibility and modularization. Platforms enabling the synchronisation of the operation of various AI agents are created and industrial components based on AI integrated in multi-agent systems are developed. One of the important aspects of intelligent production is the safe and effective cooperation of humans with industrial robots and AI systems. In this context, the authors of this article consider issues related to the type and scope of processed data, processing of mixed data sets and the phenomenon of data re-personalization, the scope of the right to privacy and issues related to automated decision making. They also indicate new or planned legal regulations that may affect intelligent production.

Keywords: intelligent manufacturing, Industry 4.0, artificial intelligence, data, data management

Wstęp

Przemysł europejski buduje przewagę konkurencyjną na rynkach światowych dzięki wysokiej jakości produktów i ich personalizacji. W produkcji wykorzystuje coraz częściej usługi chmurowe oferujące integrację różnorodnych systemów informatycznych, przemysłowy Internet Rzeczy (tzw. IIOT) oraz systemy sztucznej inteligencji (AI). Wyzwaniem jest wciąż komunikacja pomiędzy różnymi systemami oraz uzyskanie pełnej interoperacyjności, stąd w projektach do-

tyczących Przemysłu 4.0 (Habrat, 2020) pojawiają się coraz częściej platformy umożliwiające synchronizację działania agentów AI oraz opracowywane są komponenty przemysłowe oparte na AI zintegrowanej w systemy wieloagentowe. W interfejsach człowiek–maszyna (Fruggiero i in., 2020) model wiedzy semantycznej generuje odpowiednie instrukcje dla pracownika, które nie tylko pozwalają mu na bezpieczną i efektywną współpracę z robotem przemysłowym, ale stanowią istotny wkład w wyjaśnialną AI (XAI) (Bar, 2020, s. 76).

W szczególności w kontekście tego ostatniego, tj. uczestnictwa człowieka w inteligentnym środowisku produkcyjnym (Kalateh i in., 2021), pojawiają się pytania o zakres prawa do prywatności, przetwarzanie mieszanych zbiorów danych (osobowych i nieosobowych), ryzyka związane ze zjawiskiem ponownej personalizacji danych, podstawy przetwarzania danych osobowych, oraz zautomatyzowane podejmowanie decyzji wobec osób fizycznych. Warte rozważenia jest także, w jakim zakresie i w jaki sposób na inteligentną produkcję wpłyną nowe regulacje UE dotyczące danych i AI, zwłaszcza rozporządzenie 2022/868 z 30.05.2022 r. w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi – Data Governance Act, DGA)[2], projektowane rozporządzenie ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniające niektóre akty ustawodawcze Unii (akt w sprawie sztucznej inteligencji – Artificial Intelligence Act, AIA)[3] oraz rozporządzenie w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych – Data Act, DA)[4].

Dane nieosobowe, mieszane zbiory danych i ryzyko ponownej personalizacji

Jednym z podstawowych wyzwań inteligentnej fabryki, mających istotne konsekwencje prawne, jest zidentyfikowanie, jakie dane mają być przetwarzane w ramach określonego rozwiązania – czy to lokalnego agenta AI, czy to platformy z komponentami w chmurze obliczeniowej lub w ramach IIoT. Dane zbierane i generowane w środowisku produkcyjnym są bowiem bardzo zmienne i czasem nieprzewidywalne pod względem zarówno zawartości informacji (treści), jakości, jak i objętości (Sabet, 2021).

W większości przypadków w inteligentnym przemyśle będziemy mieli do czynienia z tzw. danymi maszynowymi, które należy rozumieć jako informacje w postaci cyfrowej tworzone przez aktywność komputerów, systemów IT, w tym opartych na AI, oraz innych urządzeń sieciowych. Przykładami danych maszynowych są logi aplikacji i serwerów, dane z czujników. W sensie prawnym będą to dane nieosobowe w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej[5] (dalej jako rozporządzenie 2018/1807). Dane nieosobowe można podzielić na dwie kategorie w zależności od ich źródła (KE, 2019):

1) dane, które pierwotnie nie odnosiły się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, takie jak dane dotyczące potrzeb w zakresie konserwacji maszyn przemysłowych;

2) dane, które pierwotnie były danymi osobowymi, ale poddano je następnie anonimizacji, czyli procesowi nieodwracalnego usunięcia cech wiążących daną informację ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną (zob. motyw 26 rozporządzenia 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej także jako RODO)[6].

Informacje te zazwyczaj są łączone z innymi typami danych przedsiębiorstwa, np. w celu przeprowadzania analiz efektywności produkcji lub w celu konserwacji predykcyjnej, gdzie dane maszynowe dotyczące wydajności maszyn są analizowane w czasie zbliżonym do rzeczywistego w połączeniu z danymi historycznymi dotyczącymi działania maszyn, aby przewidzieć ewentualne problemy związane ze zużyciem sprzętu i podjąć działania konserwacyjne lub naprawcze, zanim urządzenie się zepsuje. Dane maszynowe mogą być łączone z danymi osobowymi, np. w sytuacji, gdy raport z kontroli jakości na linii produkcyjnej pozwala na powiązanie danych o stanie maszyny z poszczególnymi pracownikami fabryki.

Dane są rejestrowane przez czujniki zarówno z maszyn, jak i z urządzeń noszonych przez operatorów, takich jak inteligentne rękawiczki czy okulary AR (Carmigniani & Furht, 2011). Urządzenia ubieralne wymagają szczególnej uwagi, gdyż ich czujniki mogą rejestrować ogromne ilości danych osobowych – począwszy od lokalizacji noszącej je osoby po jej przyzwyczajenia i zachowania; zapisują też informacje o wzorcach użytkowania, które mogą być osobistym „identyfikatorem". Do gromadzenia danych osobowych może dojść w sposób niezamierzony przy wykorzystaniu dronów do monitorowania infrastruktury inteligentnej fabryki, badań topograficznych i inspekcji środowiskowych terenu.

W każdym z opisanych wyżej wypadków będziemy mieli do czynienia z tzw. mieszanymi zbiorami danych, czyli z takimi ich zestawami, które obejmują zarówno dane osobowe, jak i nieosobowe. Jeśli w zbiorze danych dane osobowe i nieosobowe są nierozerwalnie związane, zastosowanie znajdzie RODO ze wszystkimi tego konsekwencjami, m.in. w zakresie podstaw prawnych przetwarzania i obowiązków administratora lub podmiotu przetwarzającego oraz zapewnienia bezpieczeństwa odpowiedniego do ryzyka związanego z przetwarzaniem. Nie ma przy tym znaczenia, czy informacje te są zapisywane i przechowywane przez jakiś czas, czy też na bieżąco nadpisywane. Samo zbieranie tych danych i nawet krótkotrwałe wykorzystanie (np. w odniesieniu do monitorowania stanu zdrowia pracownika obsługującego skomplikowaną maszynę) będzie kwalifikować się jako przetwarzanie w rozumieniu RODO.

Pojęcie „nierozerwalności" zbiorów danych osobowych i nieosobowych nie zostało zdefiniowane ani wyjaśnione

w rozporządzeniu 2018/1807. Użyte w art. 2 ust. 2 tego aktu sformułowanie: „W przypadku, gdy w zbiorze danych dane osobowe i nieosobowe są nierozerwalnie związane […]" nie wskazuje, czy odnosi się to bezpośrednio do zbiorów, w których nie jest możliwe rozdzielenie danych osobowych i nieosobowych, czy też odnosi się do dynamicznego charakteru danych osobowych (Graef i in., 2018, s. 7; Bar & Skibicki, 2019, s. 7). W wytycznych KE jako przykład ilustrujący zbiór danych obejmujący zarówno dane nieosobowe, jak i osobowe, które są „nierozerwalnie związane", podaje się sytuację, w której przedsiębiorstwo działające w UE oferuje swoje usługi za pośrednictwem elektronicznej platformy. Współpracujące przedsiębiorstwa przesyłają na tę platformę swoje dokumenty zawierające mieszane zbiory danych (np. umowy, faktury). Systemem, w którym mamy do czynienia z mieszanymi zbiorami danych, jest także tzw. CRM – system do zarządzania relacjami z klientami i raportowania sprzedaży. Rozdzielenie w nim danych osobowych od nieosobowych jest zapewne możliwe, ale byłoby nieefektywne i nieopłacalne. Podzielenie zbioru prawdopodobnie znacząco zmniejszyłoby również wartość zbioru danych.

Niezależnie od kwestii „nierozerwalnego" charakteru zbioru danych problem z kwalifikacją prawną danych w złożonym środowisku inteligentnej fabryki jest szerszy, gdyż cecha „osobowego" charakteru informacji nie jest nigdy „przypisywalna" z góry i na stałe, przez co niemożliwe jest ustalenie katalogu zamkniętego danych osobowych (Litwiński i in., 2018, s. 182; Sakowska-Baryła, 2018; Mednis, 1999, s. 35), a tym samym niemożliwe jest ustalenie takiego katalogu w odniesieniu do danych nieosobowych. W polskiej doktrynie tę cechę danych osobowych określono mianem „relatywizacji danych osobowych" (Litwiński i in., 2018, s. 182; Zimny, 2001, s. 3), natomiast w piśmiennictwie anglojęzycznym zjawisko to opisuje się jako „dynamiczną naturę pojęcia danych osobowych" (Graefi in., 2018, s. 4–5) lub „kontekstowość danych osobowych" (Gellert, 2021).

Dane nieosobowe mogą też przekształcić się w dane osobowe za pomocą inteligentnych narzędzi. Pełna anonimizacja „dziś" niekoniecznie musi być skuteczna w przyszłości, ponieważ rozwój analityki danych i sztucznych sieci neuronowych pozwala na coraz dokładniejszą identyfikację, nawet na podstawie skąpych informacji (Blackman & Forge, 2017, s. 22). Ocena, czy dane zanonimizowano prawidłowo, zależy od konkretnych okoliczności danego przypadku (Irti, 2021, s. 49–57). Zgodnie z motywem 26 RODO, aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, a także postęp technologiczny (Finck & Pallas, 2020, s. 14). Ustalenie, czy osoba fizyczna jest możliwa do zidentyfikowania, wymaga przyjrzenia się wszystkim środkom, co do których istnieje uzasadnione prawdopodobieństwo, że mogą zostać wykorzystane przez administratora lub inną osobę w celu identyfikacji osoby fizycznej w sposób bezpośredni lub pośredni (Grupa Robocza Art. 29, 2014, s. 9). Ponadto niedawne badania potwierdzają, że nawet, wydawałoby się, anonimowe zbiory danych często pozwalają na identyfikację konkretnych osób fizycznych (Rocher i in., 2019).

Odrębnym zagadnieniem, któremu warto się przyjrzeć, są kwestie wymogów co do jakości danych. Gdy chodzi o dane osobowe, zgodnie z wprowadzoną przez art. 5 ust. 1 lit. d RODO zasadą prawidłowości dane muszą być prawidłowe i w razie potrzeby uaktualniane, a administrator ma obowiązek podjęcia wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. W projekcie AIA znajdziemy jednak przepis odnoszący się do wszelkiego rodzaju danych – treningowych, walidacyjnych i testowych – wykorzystywanych w systemach AI wysokiego ryzyka, czyli takich systemów, które stanowią znaczne zagrożenie dla zdrowia i bezpieczeństwa lub praw podstawowych człowieka. Zbiory tych danych muszą być adekwatne, reprezentatywne, wolne od błędów i kompletne. Powinny one również charakteryzować się odpowiednimi właściwościami statystycznymi, w tym w odniesieniu do osób lub grup osób, wobec których system AI wysokiego ryzyka ma być wykorzystywany. W szczególności zbiory danych treningowych, walidacyjnych i testowych powinny uwzględniać – w zakresie wymaganym w świetle ich przeznaczenia – cechy, właściwości lub elementy, które są specyficzne dla określonego kontekstu geograficznego, behawioralnego lub funkcjonalnego lub okoliczności, w których system AI ma być wykorzystywany (art. 10 ust. 3). Kompromisowy tekst prezydencji francuskiej z 17.01.2022 r. złagodził te wymogi, wychodząc z założenia, że całkowita wolność od błędów może być nieosiągalna, i wprowadzając wymóg zapewnienia, by dane były możliwie wolne od błędów. W takim brzmieniu też przepis ten został uwzględniony we wspólnym stanowisku Rady w sprawie AIA (Rada UE, 2022).

Wyzwania związane z przetwarzaniem danych osobowych

W inteligentnej fabryce gromadzonych jest i generowanych mnóstwo danych osobowych, w tym danych szczególnych kategorii, o których mowa w art. 9 RODO. Jednocześnie w odniesieniu do przetwarzania danych osobowych RODO wprowadza zasadę minimalizacji danych, zgodnie z którą dane osobowe powinny być adekwatne, odpowiednie do celu przetwarzania oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Mając na względzie, że systemy AI zazwyczaj wymagają bardzo dużych ilości danych do dokonywania dokładnych predykcji (np. co do stanu maszyny i konieczności jej konserwacji) i podejmowania trafnych decyzji (np. o złożeniu zamówienia), na pierwszy rzut oka wydaje się, że zasada minimalizacji jest niezwykle trudna do zastosowania w inteligent-

nym środowisku produkcyjnym. Jednakże zasady minimalizacji nie możemy stosować w oderwaniu od innych zasad, w szczególności zasady ograniczenia celu. Zasada minimalizacji danych nie oznacza zatem, że administrator ma przetwarzać jak najmniej danych osobowych. Kluczowe jest to, że przetwarza on dane osobowe, których rzeczywiście potrzebuje do założonego celu. Sposób, w jaki zostanie podjęta decyzja o tym, jakie dane są „odpowiednie, stosowne i ograniczone do celu przetwarzania", będzie oczywiście zależał od okoliczności konkretnego przypadku.

W doktrynie zwraca się uwagę na to, że „wymóg niezbędności należy odczytywać łącznie z wymogiem adekwatności i stosowności, co powinno pozwolić na uwzględnienie okoliczności i dopuszczenie przetwarzania danych, które w istotny sposób mogą pomóc osiągnąć cele przetwarzania. W praktyce często zdarza się, że cel można osiągnąć łatwiej, szybciej i taniej, wykorzystując dane, bez których osiągnięcie podstawowego celu jest możliwe. Przyjęcie restrykcyjnej wykładni uniemożliwiałoby przetwarzanie jakichkolwiek innych danych niż tylko te, bez których cel nie może zostać osiągnięty" (Fajgielski, 2021). W wyroku z 7.08.2020 r. WSA w Warszawie uznał, że: „Użyte w przepisie art. 5 ust. 1 lit. c RODO określenie *adekwatne* oznacza *odpowiednie, zgodne, proporcjonalne, nienadmierne* i może być traktowane jako synonim słowa *stosowne*. Adekwatność i stosowność rozumieć można jako konieczność zachowania odpowiednich proporcji zakresu danych do celów przetwarzania i przetwarzanie tylko takich danych, które są potrzebne dla realizacji określonych celów"[7].

Wyzwaniem może okazać się wymóg, aby konkretne cele przetwarzania danych osobowych były każdorazowo wyraźne, uzasadnione i określone już w momencie zbierania danych. „Niezgodne z tym wymogiem byłoby np. zbieranie danych dla realizacji bliżej nieoznaczonych celów (np. stwierdzenie »przetwarzanie danych dla ważnych celów administratora« bez sprecyzowania, o jakie konkretne cele chodzi), jak również gromadzenie danych bez wskazania celu, z nastawieniem, że kiedyś dane mogą się przydać" (Fajgielski, 2021). Zasada celowości ma szczególne znaczenie w kontekście przetwarzania danych w dużych zbiorach (Drobek, 2014).

Praktyczne zastosowanie zasad ochrony danych w fazie projektowania i domyślnej ochrony danych, wdrożenie systemu zarządzania ryzykiem oraz rzetelne prowadzenie rejestru czynności przetwarzania ułatwi identyfikację tych celów i zastosowanie adekwatnych technik minimalizacji. Podkreślenia przy tym wymaga, że zasada minimalizacji danych przetwarzanych w systemach AI powinna być na etapie uczenia systemu realizowana inaczej niż na etapie jego „produkcyjnego" wykorzystania. Kiedy system AI uczy się, wówczas im więcej danych ma, tym bardziej będzie dokładny statystycznie, tj. tym bardziej prawdopodobne jest, że przechwyci każdą podstawową statystycznie użyteczną zależność między cechami w zbiorach danych. Jednocześnie jednak im więcej danych jest zbieranych na temat każdej osoby i im więcej osób, których dane znajdują się w zbiorze danych, tym większe ryzyko dla tych osób, nawet jeśli dane są zbierane w jednym konkretnym celu. Jeżeli zatem wystarczającą dokładność działania systemu można osiągnąć przy mniejszej liczbie danych lub mniejszej liczbie osób, których dane dotyczą, liczba danych lub osób powinna być ograniczona (UK Information Comissioner's Offiice, 2023).

Na etapie wdrożenia ryzyko związane z przetwarzaniem dużych ilości danych osobowych lub danych osobowych dużej liczby osób może ograniczać także stosowana w przedsiębiorstwie polityka retencji, zgodnie z zasadą ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO). Wymogu czasowego ograniczenia przetwarzania nie sposób uznać za spełniony w przypadku ograniczenia identyfikacji poprzez oddzielenie informacji identyfikujących osoby od pozostałych informacji i przechowywania danych identyfikacyjnych oddzielnie (pseudonimizacja) (Fajgielski, 2021).

W większości przypadków korzystanie z systemów AI będzie wiązało się z przetwarzaniem, które może skutkować wysokim ryzykiem naruszenia praw i wolności osób fizycznych, a co za tym idzie – rodzić prawny obowiązek dokonania oceny skutków dla ochrony danych (DPIA) zgodnie z art. 35 RODO. Wykonanie DPIA będzie w szczególności niezbędne, jeśli wykorzystanie AI lub innych technologii w inteligentnej fabryce jest związane z:

- systematyczną i kompleksową oceną aspektów osobowych z wykorzystaniem zautomatyzowanego przetwarzania, w tym profilowania, na podstawie którego podejmowane są decyzje wywołujące skutki prawne lub podobnie istotne; lub
- przetwarzaniem na dużą skalę szczególnych kategorii danych osobowych.

DPIA będzie również konieczna w przypadku, gdy technologie stosowane w środowisku produkcyjnym zbierają dane z różnych źródeł (np. z kamer, dronów i czujników), śledzą lokalizacje lub zachowania (np. poprzez urządzenia ubieralne) lub dokonują oceny lub punktacji (np. oceny jakości pracy danej osoby). Wykonanie DPIA powinno dać administratorowi dowody na to, że rozważono mniej ryzykowne alternatywy, za pomocą których można osiągnąć ten sam cel przetwarzania, i uzasadnić, dlaczego wybrano np. system AI zamiast alternatywnych technologii. Jest to szczególnie ważne w przypadku korzystania z art. 6 ust. 1 lit. f RODO jako podstawy prawnej przetwarzania.

Przy ustalaniu podstaw prawnych przetwarzania danych osobowych w systemach AI zaleca się oddzielenie fazy badawczo-rozwojowej (w tym konceptualizacji, projektowania, szkolenia i doboru modeli) od fazy wdrożeniowej. Są to odrębne procesy, w których pojawiają się odrębne cele przetwarzania, z różnymi zagrożeniami dla osób, których dane dotyczą. Dobrym przykładem może być tu system AI, który jest opracowywany jako system ogólnego przeznaczenia (np. do rozpoznawania obrazu), a następnie wdrażany w różnych kontekstach do różnych celów jako system rozpoznawania twarzy używany do:

1) zapobiegania przestępczości,
2) uwierzytelniania,
3) oznaczania znajomych w sieciach społecznościowych.

Każde z tych zastosowań wymaga innej podstawy prawnej. Duże trudności może sprawiać stosunkowo szeroki zakres danych szczególnych kategorii. Po pierwsze, wchodzi tu w grę kwestia adekwatności przetwarzania tych danych do celów przyjętych przez administratora, a po drugie – podstawa prawna przetwarzania. Odnośnie do tego pierwszego zagadnienia należy rozważyć, na ile wykorzystywanie np. danych biometrycznych jest konieczne i adekwatne dla osiągnięcia celu w postaci kontroli czasu pracy albo danych dotyczących zdrowia pracownika – do mierzenia jego wydajności[8].

Większym jednak problemem wydaje się być to, że przetwarzanie danych wrażliwych jest co do zasady zabronione, a RODO dopuszcza je tylko w wyjątkowych przypadkach określonych precyzyjnie w przepisie art. 9 ust. 2 RODO (np. wyraźna zgoda lub szczególne przepisy prawa). Co więcej, postęp w uczeniu maszynowym pozwala systemom AI na jeszcze łatwiejsze i bardziej precyzyjne wykrywanie wzorców w pozornie niepowiązanych danych. Administrator danych korzystający z systemu AI opartego na uczeniu maszynowym musi stale monitorować, czy system ten nie przetwarza danych osobowych szczególnych kategorii w celu sporządzania prognoz (np. w ramach oceny pracowników). Jeżeli system AI rzeczywiście wyciąga wnioski na podstawie danych szczególnych kategorii, konieczne jest posiadanie podstawy przetwarzania na podstawie art. 9 RODO, niezależnie od tego, czy takie przetwarzanie było zamierzone, czy też nie.

W projekcie AIA pojawia się nowa podstawa dla przetwarzania danych wrażliwych. Zgodnie z art. 10 ust. 5 AIA w zakresie, w jakim jest to ściśle niezbędne do celów zapewnienia monitorowania, wykrywania i korygowania tendencyjności systemów sztucznej inteligencji wysokiego ryzyka, dostawcy takich systemów mogą przetwarzać szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO. Warunkiem legalności takiego przetwarzania będzie zastosowanie odpowiednich zabezpieczeń gwarantujących ochronę podstawowych praw i wolności osób fizycznych.

Opisane wyżej łączenie danych osobowych z danymi ze środowiska produkcyjnego może prowadzić do tworzenia profili i być podstawą do zautomatyzowanego podejmowania decyzji wobec podmiotów danych. Wprowadzony przez RODO w art. 22 generalny zakaz podejmowania automatycznych decyzji wobec podmiotów dotyczy wyłącznie profilowania kwalifikowanego, czyli takiego, które prowadzi do zautomatyzowanych decyzji o skutku prawnym lub podobnie istotnym. Jeżeli nie mamy do czynienia z takim skutkiem automatycznych decyzji, w grę wchodzi tzw. profilowanie zwykłe, którego regulacja ogranicza się do możliwości wniesienia sprzeciwu przez osobę, której dane dotyczą (art. 21 RODO).

Od zakazu, o którym mowa w art. 22 RODO, wprowadzono trzy wyjątki, a zatem zakaz nie ma zastosowania, jeśli decyzja:

- jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
- jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
- opiera się na wyraźnej zgodzie osoby, której dane dotyczą (Mednis, 2019).

W inteligentnych fabrykach częściowo lub całkowicie autonomiczne systemy już obejmują, a będą obejmować w coraz większym zakresie, także zarządzanie personelem. Nie można więc wykluczyć, że zastosowanie znajdzie w takich przypadkach art. 22 RODO. Administrator powinien w takim przypadku zadbać o należyte poinformowanie o takim przetwarzaniu (w tym o zastosowanej logice, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą) i przeprowadzać regularne kontrole w celu sprawdzenia, czy system AI działa zgodnie z przeznaczeniem. Jeżeli automatyczne podejmowanie decyzji jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem albo gdy odbywa się na podstawie wyraźnej zgody, administrator danych powinien wdrożyć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej zapewnić prawo do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. W praktyce oznacza to konieczność zapewnienia osobie, której dane dotyczą, możliwości odwołania się od automatycznej decyzji, a odwołanie takie powinno być rozpatrzone przez człowieka.

W tym kontekście istotne jest zapewnienie należytego wyjaśnienia decyzji, która wywołuje wobec osoby skutki prawne lub podobnie istotne. Przede wszystkim:

- system AI powinien przedstawić alternatywny wynik pokazujący, jak uzyskany wynik (w postaci prognozy lub decyzji) różni się od innych potencjalnych wyników;
- w wyjaśnieniu należy przedstawić kontekst, w jakim działa AI, w tym m.in. informacje o danych wykorzystywanych do trenowania modelu;
- wyjaśnienie powinno wskazywać, czy dany przypadek jest „odstający" i bardzo różni się od danych użytych do trenowania modelu (to zidentyfikuje sytuację, w której system AI działa błędnie i wymaga interwencji człowieka);
- wyjaśnienie powinno być dostępne w czasie rzeczywistym, ale dopuszczalne jest również złożenie wyjaśnień w rozsądnym terminie po wydaniu decyzji, o ile umożliwi to osobie zainteresowanej skorzystanie z prawa do odwołania się od decyzji AI (Bar, 2020).

W przypadku niewystarczającej wiedzy lub danych system AI powinien poinformować o tym fakcie, co powinno zablokować automatyczne podjęcie decyzji.

Zarządzanie danymi i udostępnianie danych

Na danych różnego rodzaju opiera się większość innowacji w UE i znajdują się one w centrum transformacji cyfrowej (KE, 2020, s. 1). Prawdziwym wyzwaniem dla UE jest

stworzenie dobrze działającego mechanizmu, umożliwiającego wykorzystanie danych wysokiej jakości, które będą mogły podlegać swoistemu recyklingowi w wielu różnych organizacjach (KE, 2020, s. 1). Tym, co ma dać UE przewagę nad resztą świata, jest wprowadzenie do unijnego prawa jakościowych i przy tym eksperymentalnych narzędzi prawnych: aktu w sprawie zarzadzania danymi (DGA) oraz aktu o danych (DA).

Z punktu widzenia wykorzystania danych w inteligentnej fabryce w DGA można wyróżnić trzy podstawowe zagadnienia: wykorzystanie danych będących w posiadaniu podmiotów sektora publicznego do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie, usługi pośrednictwa danych oraz altruizm danych.

Jeśli chodzi o dane (rozumiane szeroko jako wszelkie cyfrowe odwzorowania działań, faktów lub informacji oraz wszelkie kompilacje takich działań, faktów lub informacji, w tym w formie zapisu dźwiękowego, wizualnego lub audiowizualnego) będące w posiadaniu podmiotów sektora publicznego, możliwe jest skorzystanie, poza danymi „zwykłymi", również z danych chronionych ze względu na poufność informacji handlowej, ochronę własności intelektualnej, ochronę danych osobowych, a nawet poufność informacji statystycznych (art. 3 ust. 1 DGA). Co do zasady dane mogą te być udostępniane przez ustanowione w tym celu podmioty sektorowe (art. 7 DGA). Ponowne wykorzystanie danych ma być stosowane jak najszerzej, dlatego zakazane jest zawieranie umów czy stosowanie praktyk prowadzących do przyznania wyłączności do wykorzystania takich danych na potrzeby ponownego ich wykorzystania (art. 4 ust. 1 DGA) oraz będzie odbywało się na podstawie wniosku zainteresowanego, złożonego do właściwego podmiotu sektora publicznego. Warunki wykorzystania tych danych muszą być udostępnione publicznie (art. 5 ust. 1 DGA). Winny być one przejrzyste, niedyskryminujące, proporcjonalne i obiektywnie uzasadnione (art. 5 ust. 2 DGA). Nadto, gdy nie można zezwolić na ponowne wykorzystanie danych i nie ma podstawy prawnej do ich przetwarzania na gruncie RODO, podmiot sektora publicznego ma dołożyć wszelkich starań, by pomóc podmiotom prywatnym w uzyskaniu prawidłowych zgód na przetwarzanie i wykorzystanie takich danych (art. 5 ust. 6 DGA). Uzyskanie danych we wspomniany sposób może odbywać się odpłatnie (art. 6 ust. 1 DGA). Kluczową kwestią jest, na ile podmioty publiczne będą posiadały dane odpowiedniej jakości, tak by były one najbardziej przydatne w nowoczesnym przemyśle.

Kolejnym ważnym *novum* legislacyjnym jest wprowadzenie „usług pośrednictwa danych", które mają na celu ustanowienie – za pomocą środków technicznych, prawnych lub innych – stosunków handlowych między – z jednej strony – nieokreśloną liczbą osób, których dane dotyczą, i posiadaczy danych oraz – z drugiej strony – użytkownikami danych, do celów dzielenia się danymi, w tym do celów wykonywania praw osób, których dane dotyczą, w odniesieniu do danych osobowych (art. 2 pkt. 11 DGA). Świadczenie usług pośrednictwa danych wymaga zgłoszenia do właściwego organu (art. 10–11 DGA), a pośrednik nie może wykorzystywać danych w jakimkolwiek innym celu niż do dyspozycji użytkowników danych (art. 12 lit. a DGA) (Grafenstein, 2022). Zastosowanie przepisu dotyczącego usług pośrednictwa danych jest wyłączone m.in. dla usług:

1) w ramach których dane są pozyskiwane od posiadaczy danych i agregowane, wzbogacane lub przekształcane w celu dodania im znaczącej wartości, a następnie użytkownikom danych udzielana jest licencja na wykorzystanie uzyskanych w ten sposób danych bez ustanawiania stosunku handlowego między nimi a posiadaczami danych;

2) z których korzysta wyłącznie jeden dysponent danych w celu umożliwienia wykorzystywania danych będących w jego posiadaniu, lub usług, z których korzysta wiele osób prawnych w zamkniętej grupie, w tym w ramach stosunków z dostawcami lub klientami lub współpracy nawiązanej na podstawie umowy, w szczególności usług, których głównym celem jest zapewnienie funkcjonalności przedmiotów i urządzeń podłączonych do IoT.

Ważnym problemem okazuje się zatem interpretacja wspomnianego wyłączenia dla dostawców usług powiązanych z IoT. Z jednej strony brak takiej kwalifikacji będzie się dla nich wiązał z brakiem konieczności spełnienia wymogów legislacyjnych (np. w zakresie zgłoszenia czy warunków świadczenia). Z drugiej jednak taka działalność prowadzona bez zezwolenia może zostać zagrożona sankcjami w prawodawstwie krajowym na podstawie art. 34 DGA. Prawidłowe uregulowanie tej kwestii będzie zatem stanowiło poważne wyzwanie dla ustawodawstwa krajowego.

Istotną instytucją prawną regulowaną przez DGA jest także altruizm danych (art. 16 DGA), czyli dobrowolne dzielenie się danymi:

1) na podstawie wyrażonej przez osoby, których dane dotyczą, zgody na przetwarzanie dotyczących ich danych osobowych lub

2) na podstawie udzielonego przez posiadaczy danych pozwolenia na wykorzystywanie ich danych nieosobowych, bez żądania ani otrzymania za to wynagrodzenia wykraczającego poza zwrot kosztów poniesionych przez te osoby lub posiadaczy w związku z udostępnieniem ich danych.

Dzielenie się danymi ma następować na podstawie przepisów prawa krajowego do celów leżących w interesie ogólnym w obszarach takich jak opieka zdrowotna, zwalczanie zmiany klimatu, poprawa mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk urzędowych, poprawa świadczenia usług publicznych, kształtowanie polityki publicznej lub do celów badań naukowych. Kluczowe znaczenie zyskuje zatem konstrukcja pojęcia „interesu ogólnego" (BEUC, 2021, s. 4, 8). Mając na uwadze dokonane wyliczenie potencjalnych spraw mieszczących się w tym pojęciu, w tym zwłaszcza zwalczanie zmian klimatu i poprawę mobilności, wydaje się, że celem ogólnym może być szeroko rozumiany postęp techniczny. Ponownie zatem to od prawodawcy krajowego będzie zależała możliwość skorzystania z dobrodziejstw „altruizmu danych" przez inteligentny przemysł.

DGA, choć z jednej strony przełomowy dla realizacji Europejskiej strategii w zakresie danych, z drugiej prowokuje pytanie o to, czy rzeczywiście istnieje popyt ze strony podmiotów danych na usługi świadczone poprzez określone

w tym akcie modele biznesowe na tyle, by DGA okazał się udanym „przedsięwzięciem" (Leistner, 2021, s. 2, 10; Carovano & Michele, 2023, s. 24; Michałowicz, 2022).

Podobnie jak DGA, także akt o danych ma na celu ustanowienie przepisów dotyczących udostępniania danych. Przyszła regulacja DA ma służyć ułatwieniu dostępu do danych generowanych w wyniku korzystania z produktu lub powiązanej usługi użytkownikom tego produktu lub tej usługi, a także wesprzeć udostępnianie danych przez posiadaczy danych odbiorcom danych oraz organom sektora publicznego, instytucjom, agencjom lub organom UE (art. 1 ust. 1 DA).

W przypadku inteligentnych fabryk kluczowe znaczenie zdaje się mieć art. 3 DA, który wymaga, by projektowane i wytwarzane produkty wraz z ich usługami towarzyszącymi były tworzone w taki sposób, aby dane generowane w wyniku korzystania z nich były domyślnie łatwo, bezpiecznie oraz – w razie potrzeby i w stosownych przypadkach – bezpośrednio dostępne dla użytkownika (art. 3 ust. 1 DA). Będzie się to wiązać także z koniecznością spełnienia dodatkowego obowiązku informacyjnego przed zawarciem umowy dotyczącej zakupu, najmu lub leasingu takiego produktu (art. 3 ust. 2 DA) oraz z zapewnieniem użytkownikom dostępu do danych z produktu (art. 4 ust. 1 DA). Warto zauważyć, że DA wpłynie także w sposób istotny na prawa *sui generis* dotyczące baz danych z art. 7 dyrektywy 96/9/WE. Aktualne brzmienie projektu wskazuje bowiem, że prawo *sui generis*, o którym mowa w dyrektywie w sprawie baz danych (dyrektywa 96/9/WE), nie ma zastosowania do baz danych zawierających dane wygenerowane lub pozyskane wskutek korzystania z produktów lub powiązanych usług, zatem prawo *sui generis* nie będzie kolidowało z prawami przedsiębiorstw i konsumentów dotyczącymi dostępu do danych, korzystania z danych i ich udostępniania przewidzianymi w DA. W doktrynie krytykuje się takie rozwiązanie, wskazując, że obecna redakcja tego przepisu wyłącza w tym zakresie regulację dotyczącą baz danych spod unijnego prawa, co umożliwia wprowadzenie prawodawcom krajowym odrębnych regulacji w tym zakresie (Husovec i in., 2022).

W chwili obecnej DA znajduje się w trakcie procesu legislacyjnego, wobec czego jego postanowienia mogą się znacząco zmienić. Jest to o tyle możliwe, że projektowi zarzucono brak spójności, co wynika z próby pogodzenia różnych interesów – wzmocnienia praw użytkownika oraz wsparcia konkurencyjności i innowacyjności europejskich przedsiębiorstw (Colangelo, 2022, s. 15; Kerber, 2022; Leistner & Antoine, 2022, s. 69–121).

Podsumowanie

UE przeżywa prawdziwą legislacyjną rewolucję cyfrową, będąc w wielu aspektach pionierem i wzorcem postępowania na skalę światową (Bradford, 2012). Nowe regulacje niewątpliwie wpłyną na inteligentną produkcję, w szczególności w zakresie szeroko pojętego zarządzania danymi i dzielenia się nimi w ramach europejskich przestrzeni danych.

Szczególnej uwagi już dziś wymagają mieszane zbiory danych, których wykorzystanie jest niejasne pod względem regulacyjnym. Z tej przyczyny w doktrynie europejskiej pojawił się postulat wprowadzenia zasad wyłączenia odpowiedzialności (tzw. bezpiecznych przystani) dla dostawców usług dokonujących transakcji dotyczących mieszanych zbiorów danych, warunkowany zastosowaniem anonimizacji na rozsądnym poziomie (Picht & Richter, 2021, s. 14). Wydaje się, że takie rozwiązanie ułatwiłoby zgodne z prawem wykorzystanie mieszanych zbiorów danych w inteligentnej fabryce.

W przyszłości możemy się też spodziewać wzmocnienia praw użytkowników końcowych wobec danych generowanych przez używane przez nich inteligentne urządzenia. Szeroko rozumiana suwerenność danych to słuszny kierunek, jednak prawa w tym zakresie powinny być równoważone przez regulacje wspierające innowacyjność i konkurencyjność europejskiego przemysłu oraz branży przemysłowego Internetu Rzeczy.

Przypisy/Notes

[1] Artykuł powstał w ramach projektu *Multi-Agent Systems for Pervasive Artificial Intelligence for Assisting Humans in Modular Production Environments (MAS4AI)* finansowanego ze środków Unii Europejskiej w ramach HORIZON 2020 *Industrial Leadership – Leadership in enabling and industrial technologies – Information and Communication Technologies (ICT)*.

[2] Dz. Urz. UE L 152, 3.06.2022 r., s. 1–44.

[3] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze unii, COM(2021) 206.

[4] Wniosek 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.

[5] Dz. Urz. UE 303, 28.11.2018, s. 59–68.

[6] Dz. Urz. UE L 119, 4.05.2016, s. 1–88.

[7] Wyrok WSA w Warszawie z 7.08.2020, II SA/Wa 809/2.

[8] Wyrok NSA z 1.12.2009, I OSK 249/09.

Bibliografia/References

Literatura/Literature

Bar, G. (2020). Przejrzystość, w tym wyjaśnialność, jako wymóg prawny dla systemów Sztucznej Inteligencji. *Monitor Prawniczy*, (20), dodatek specjalny.

Bar, G., & Skibicki, R. (2019). Mieszane zbiory danych. *Magazyn ODO. Ochrona Danych Osobowych*, (9).

BEUC. (2021). *Data Governance Act. BEUC position paper*. Ref: BEUC-X-2021-026, 23.03.2021. BEUC. The European Consumer Organisation.

Biernacki, W., & Michałowicz, A. (2022). Zwiększanie wymiany danych w Unii Europejskiej w świetle projektu aktu w sprawie zarządzania danymi. *Europejski Przegląd Sądowy*, (1).

Blackman, C., & Forge, S. (2017). *Data flows – future scenarios: In-depth analysis for the ITRE Committee*. www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_ENpdf

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, *107*(1).

Carmigniani, J., & Furht, B. (2011). Augmented reality: An overview. W: B. Furht, *Handbook of Augmented Reality*. Springer.

Carovano, G., & Michele, F. (2023). *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*.

Colangelo, G. (2022). *European proposal for a Data Act – A first assessment*. CERRE Evaluation Paper.

von Ditfurth, L., & Linemann, G. (2022). The Data Governance Act: Promoting or restricting data intermediaries? *Journal of Competition and Regulation in Network Industries*, *23*(1). https://doi.org/10.1177/17835917221141324

Drobek, P. (2014). Zasada celowości w dobie wielkich zbiorów danych (big data). *Monitor Prawniczy*, (14), dodatek, 21–28.

EROD & EIOD. (2021). Wspólna opinia EROD i EIOD 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi, wersja. 1.1.

Fajgielski, P. (2021). Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). W: P. Fajgielski (Red.), *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. Wolters Kluwer.

Finck, M., & Pallas, F. (2020). Distinguishing personal from non-personal data. *International Data Privacy Law*, *10*(1). https://doi.org/10.1093/idpl/ipz026

Fruggiero, F., Lambiase, A., Panagou, S., & Sabattini, L. (2020). Cognitive human modelling in collaborative robotics. *Procedia Manufacturing*, (51), 584–591. https://doi.org/10.1016/j.promfg.2020.10.082

Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, *11*(2), 196–208. https://doi.org/10.1093/idpl/ipaa023

Graef, I., & Gellert, R. (2021). *The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing*. TILEC Discussion Paper No. DP2021-006.

Graef, I., Gellert, R., & Husovec, M. (2018). *Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation*. TILEC Discussion Paper (2018–029). http://dx.doi.org/10.2139/ss

Grafenstein, M. (2022). *Reconciling conflicting interests in data through data governance. An analytical framework (and a brief discussion of the Data Governance Act draft, the Data Act draft, the AI Regulation draft, as well as the GDPR)*. HIIG Discussion Paper Series No. 2022–02.

Grupa Robocza Art. 29. (2014). *Opinia 05/2014 w sprawie technik anonimizacji*, 10.04.2014.

Habrat, D. (2020). Legal challenges of digitalization and automation in the context of Industry 4.0. *Procedia Manufacturing*, (51), 938–942.

Husovec, M., Sentfleben, M., Derclaye, E., & van Eechoud, M. (2022). *Opinion of the European Copyright Society on selected aspects of the proposed Data Act*. 12.05.2022.

Irti, C. (2021). Personal data, non-personal data, anonymised data, pseudonymised data, de-identified data. W: R. Senigaglia, C. Irti, & A. Bernes, *Privacy and Data Protection in Software Services, Services and Business Process Reengineering*. Springer.

Kalateh, S., Estrada-Jimenez, L. A., Pulikottil, T., Nikghadam Hojjati, S., & Barata, J. (2021). *Feeling Smart Industry*. 2nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS).

KE. (2019). Wytyczne Komisji Europejskiej dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

KE. (2020). Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia w zakresie danych.

KE. (2022). Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych).

Kerber, W. (2022). *Governance of IoT data: Why the EU Data Act will not fulfil its objectives* (second version). http://dx.doi.org/10.2139/ssrn.4080436

Leistner, M. (2021). The Commission's vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act. A critical primer. http://dx.doi.org/10.2139/ssrn.3789041

Leistner, M., & Antoine, L. (2022). *IPR and the use of open data and data sharing initiatives by public and private actors. Study requested by the JURI committee*. European Parliament.

Litwiński, P., Barta, P., & Kawecki, M. (2018). W: P. Litwiński (Red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem danych. Komentarz*. C.H.Beck.

Mednis, A. (1999). Ochrona prawna danych osobowych, a zagrożenie prywatności – rozwiązania polskie. W: M. Wyrzykowski, *Ochrona danych osobowych*. Instytut Spraw Publicznych.

Mednis, A. (2019). *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*. Presscom.

Michałowicz, A. (2022). Altruizm danych w świetle aktu w sprawie zarządzania danymi – między teorią a praktyką. *internetowy Kwartalnik Antymonopolowy i Regulacyjny*, (5). https://doi.org/10.7172/2299-5749.IKAR.5.11.3

Picht, P., & Richter, H. (2021). *The proposed EU Digital Services Regulation 2020: Data Desiderata*. Max Planck Institute for Innovation & Competition Research Paper No. 21–21.

Rada UE. (2022). *Komunikat prasowy: Akt o sztucznej inteligencji: Rada apeluje o bezpieczną sztuczną inteligencję, zgodną z prawami podstawowymi.* 6.12.2022. https://www.consilium.europa.eu/pl/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

Richter, H., & Slowinski, P. R. (2019). The data sharing economy: On the emergence of new intermediaries. *ICC – International Review of Intellectual Property and Competition Law*, *50*(1), 4–29. https://doi.org/10.1007/s40319-018-00777-7

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, (10). https://doi.org/10.1038/s41467-019-10933-3

Sabet, E. (2021). Reviewing the challenges of big data use in smart industries. *International Journal of Innovation in Management Economics and Social Science*, *1*(4), 66–72. https://doi.org/10.52547/ijimes.1.4.66

Sakowska-Baryła, M. (2018). Art. 4. W: M. Sakowska-Baryła, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. C.H.Beck.

UK Information Comissioner's Offiice. (2023). *Guidance on AI and Data Protection*. https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/

Zimny, W. (2001). Praktyczne skutki nowelizacji ustawy o ochronie danych osobowych z 25.08.2001 r. *Ochrona Danych Osobowych*. Biuletyn ABI, (21).

Orzecznictwo/Judgments

Wyrok NSA z 1.12.2009, I OSK 249/09.

Wyrok WSA w Warszawie z 7.08.2020, II SA/Wa 809/2.

Dr Gabriela Bar

Radczyni prawna, partnerka w Szostek_Bar i Partnerzy Kancelarii Prawnej. Ekspertka w zakresie umów elektronicznych, e-commerce, zastosowań AI oraz ochrony prywatności. Członkini Komitetu Prawnego IEEE w projekcie IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems; członkini Stowarzyszenia Prawa Nowych Technologii, Komisji Nowych Technologii FBE oraz Women in AI. Adiunktka na WPiA Uniwersytetu Śląskiego w Katowicach, zaangażowana w project Multi-Agent Systems for Pervasive Artificial Intelligence for Assisting Humans in Modular Production Environments (MAS4AI). Adiunktka na WPiA Uniwersytetu Opolskiego; członkini zespołu projektowego Smart Human Oriented Platform for Connected Factories (SHOP4CF).

Dr Rafał Skibicki

Doktor w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej na WPAiE Uniwersytetu Wrocławskiego, prawnik w Szostek_Bar i Partnerzy Kancelarii Prawnej, asystent na WPiA Uniwersytetu Śląskiego w Katowicach zaangażowany w projekt Multi-Agent Systems for Pervasive Artificial Intelligence for Assisting Humans in Modular Production Environments (MAS4AI). Specjalista z zakresu prawa własności intelektualnej, prawa nowych technologii, prawa umów i ochrony prywatności.

Dr Gabriela Bar

Attorney at Law, partner at Szostek_Bar i Partnerzy Kancelaria Prawna. Experienced expert in the field of electronic contracts, e-commerce, legal aspects of IT systems implementation, usage of AI and privacy protection. Member of the IEEE Legal Committee in the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems; member of the New Technologies Law Association, FBE New Technologies Commission and Women in AI. Researcher at the Silesia University in Katowice (Poland) and University od Opole; member of the legal teams in HORIZON 2020 projects: Multi-Agent Systems for Pervasive Artificial Intelligence for Assisting Humans in Modular Production Environments (MAS4AI) and Smart Human Oriented Platform for Connected Factories (SHOP4CF).

Dr Rafał Skibicki

PhD at the Center for Research on Legal and Economic Problems of Electronic Communication at the Faculty of Law of the University of Wrocław, lawyer at Szostek_Bar and Partners Legal Office, and Researcher at the Silesia University in Katowice (Poland) member of the legal team in HORIZON 2020 project: Multi-Agent Systems for Pervasive Artificial Intelligence for assisting Humans in Modular Production Environments (MAS4AI). Specialist in intellectual property law, new technology law, contract law and privacy protection.