

## III

(Akty przygotowawcze)

## KOMITET REGIONÓW

INTERACTIO – POSIEDZENIE HYBRYDOWE – 147. SESJA PLENARNA KR-U, 1.12.2021–2.12.2021

Opinia Europejskiego Komitetu Regionów – Europejskie podejście do sztucznej inteligencji – akt w sprawie sztucznej inteligencji

(zmieniona opinia)

(2022/C 97/12)

<b>Sprawozdawca:</b>	Guido RINK (NL/PES), członek zarządu gminy Emmen
<b>Dokumenty źródłowe:</b>	Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Promowanie europejskiego podejścia do sztucznej inteligencji” COM(2021) 205 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

## I. ZALECANE POPRAWKI

## Poprawka 1

Motyw 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
Celem niniejszego rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych, w szczególności w zakresie rozwoju, wprowadzania do obrotu i wykorzystywania sztucznej inteligencji zgodnie z wartościami Unii. Niniejsze rozporządzenie służy realizacji szeregu nadrzędnych celów interesu publicznego, takich jak wysoki poziom ochrony zdrowia, bezpieczeństwa i praw podstawowych, oraz zapewnia swobodny przepływ transgraniczny towarów i usług opartych na sztucznej inteligencji, uniemożliwiając tym samym państwom członkowskim nakładanie ograniczeń w zakresie opracowywania, wprowadzania do obrotu i wykorzystywania systemów sztucznej inteligencji, chyba że wyraźnie zezwolono na to w niniejszym rozporządzeniu.	Celem niniejszego rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego <b>i zagwarantowanie praw podstawowych obywateli</b> poprzez ustanowienie jednolitych ram prawnych, w szczególności w zakresie rozwoju, wprowadzania do obrotu i wykorzystywania sztucznej inteligencji zgodnie z wartościami Unii. Niniejsze rozporządzenie służy realizacji szeregu nadrzędnych celów interesu publicznego, takich jak wysoki poziom ochrony zdrowia, bezpieczeństwa i praw podstawowych, oraz zapewnia swobodny przepływ transgraniczny towarów i usług opartych na sztucznej inteligencji, uniemożliwiając tym samym państwom członkowskim nakładanie ograniczeń w zakresie opracowywania, wprowadzania do obrotu i wykorzystywania systemów sztucznej inteligencji, chyba że wyraźnie zezwolono na to w niniejszym rozporządzeniu.

**Uzasadnienie**

Odniesienie do praw podstawowych ma na celu podkreślenie związku z Kartą praw podstawowych Unii Europejskiej.

**Poprawka 2**

Nowy motyw po motywie 6

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
	<p><i>Definiowanie systemów sztucznej inteligencji jest procesem ciągłym, który uwzględnia kontekst funkcjonowania sztucznej inteligencji, dotrzymuje kroku przemianom społecznym w tej dziedzinie oraz bierze pod uwagę związek między ekosystemem doskonałości i ekosystemem zaufania.</i></p>

**Uzasadnienie**

Rozwój sztucznej inteligencji i technologii wymaga adaptacyjnego i ewoluującego podejścia. W motywie tym stwierdza się, że definicja AI powinna ewoluować wraz z wpływem czasu i stanem rozwoju systemów i zastosowań AI.

**Poprawka 3**

Motyw 20

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>W celu zapewnienia, aby systemy te były wykorzystywane w sposób odpowiedzialny i proporcjonalny, należy również zastrzec, że w każdej z tych trzech wąsko zdefiniowanych sytuacji z zamkniętej listy należy uwzględnić pewne elementy, w szczególności charakter sytuacji, która skutkowałą złożeniem wniosku, wpływ korzystania z takich systemów na prawa i wolności wszystkich zainteresowanych osób, a także zabezpieczenia i warunki przewidziane w związku z korzystaniem z takich systemów. Ponadto wykorzystanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa powinno podlegać <b>odpowiednim</b> ograniczeniom w czasie i przestrzeni, z uwzględnieniem w szczególności dowodów lub wskazówek dotyczących zagrożeń, ofiar lub sprawcy. Referencyjna baza danych osób powinna być odpowiednia dla każdego przypadku użycia w każdej z trzech wyżej wymienionych sytuacji.</p>	<p>W celu zapewnienia, aby systemy te były wykorzystywane w sposób odpowiedzialny i proporcjonalny, należy również zastrzec, że w każdej z tych trzech wąsko zdefiniowanych sytuacji z zamkniętej listy należy uwzględnić pewne elementy, w szczególności charakter sytuacji, która skutkowałą złożeniem wniosku, wpływ korzystania z takich systemów na prawa i wolności wszystkich zainteresowanych osób, a także zabezpieczenia i warunki przewidziane w związku z korzystaniem z takich systemów. <b>Przed wyjątkowym wykorzystaniem tych systemów należy przeprowadzić konsultacje z właściwymi władzami lokalnymi i regionalnymi.</b> Ponadto wykorzystanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa powinno podlegać <b>rygorystycznym</b> ograniczeniom w czasie i przestrzeni, z uwzględnieniem w szczególności dowodów lub wskazówek dotyczących zagrożeń, ofiar lub sprawcy. Referencyjna baza danych osób powinna być odpowiednia dla każdego przypadku użycia w każdej z trzech wyżej wymienionych sytuacji.</p>

**Uzasadnienie**

Nie należy lekkomyślnie wykorzystywać systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym”.

**Poprawka 4**

## Motyw 21

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Każde użycie systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa powinno podlegać wyraźnemu i szczegółowemu zezwoleniu wydanemu przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego. Takie zezwolenie należy <b>zasadniczo</b> uzyskać przed rozpoczęciem korzystania z systemu, z wyjątkiem należycie uzasadnionych sytuacji nagłych, to znaczy sytuacji, w których potrzeba skorzystania z danego systemu jest na tyle duża, że uzyskanie zezwolenia przed rozpoczęciem korzystania jest faktycznie i obiektywnie niemożliwe. W <b>takich sytuacjach nagłych</b> wykorzystanie powinno być ograniczone do absolutnie niezbędnego minimum i powinno podlegać odpowiednim zabezpieczeniom i warunkom określonym w prawie krajowym i <b>sprecyzowanym w kontekście każdego przypadku pilnego użycia przez sam organ ścigania</b>. Ponadto organ ścigania powinien <b>w takich sytuacjach</b> dążyć do <b>jak najszybszego</b> uzyskania zezwolenia, <b>podając jednocześnie powody, dla których nie mógł wystąpić o nie wcześniej</b>.</p>	<p>Każde użycie systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa powinno podlegać wyraźnemu i szczegółowemu zezwoleniu wydanemu przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego. Takie zezwolenie należy uzyskać przed rozpoczęciem korzystania z systemu, z wyjątkiem należycie uzasadnionych sytuacji nagłych, to znaczy sytuacji, w których potrzeba skorzystania z danego systemu jest na tyle duża, że uzyskanie zezwolenia przed rozpoczęciem korzystania jest faktycznie i obiektywnie niemożliwe. W <b>każdym przypadku</b> wykorzystanie powinno być ograniczone do absolutnie niezbędnego minimum i powinno podlegać odpowiednim zabezpieczeniom i warunkom określonym w prawie krajowym. Ponadto organ ścigania powinien <b>niezwłocznie powiadomić zainteresowane władze lokalne i regionalne oraz</b> dążyć do uzyskania zezwolenia <b>właściwych organów</b>.</p>

**Uzasadnienie**

Polityczno-administracyjna odpowiedzialność za zarządzanie przestrzenią publiczną i kontrolę nad nią spoczywa na władzach lokalnych i regionalnych. W związku z tym powinny one być odpowiednio zaangażowane w rozmieszczanie takich systemów w przestrzeni publicznej. W nagłych sytuacjach, w których nie można racjonalnie oczekiwać uprzednich konsultacji, dany organ lokalny lub regionalny powinien zostać niezwłocznie poinformowany o wykorzystaniu systemów biometrycznych w przestrzeni publicznej.

## Poprawka 5

Motyw 39

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Systemy sztucznej inteligencji wykorzystywane w zarządzaniu migracją, azylem i kontrolą graniczną mają wpływ na osoby, które często znajdują się w szczególnie trudnej sytuacji i które są zależne od rezultatów działań właściwych organów publicznych. Dokładność, niedyskryminujący charakter i przejrzystość systemów sztucznej inteligencji wykorzystywanych w tych kontekstach są zatem szczególnie istotne w celu zapewnienia poszanowania praw podstawowych zainteresowanych osób, w szczególności ich prawa do swobodnego przemieszczania się, niedyskryminacji, ochrony życia prywatnego i danych osobowych, ochrony międzynarodowej i dobrej administracji. Za systemy wysokiego ryzyka <b>należy</b> zatem uznać systemy sztucznej inteligencji przeznaczone do wykorzystywania przez właściwe organy publiczne odpowiedzialne za wykonywanie zadań w dziedzinach zarządzania migracją, azylem i kontrolą graniczną jako poligrafy i podobne narzędzia lub do wykrywania stanu emocjonalnego osoby fizycznej; w celu oceny niektórych zagrożeń stwarzanych przez osoby fizyczne wjeżdżające na terytorium państwa członkowskiego lub ubiegające się o wizę lub azyl; w celu weryfikacji autentyczności odpowiednich dokumentów osób fizycznych; w celu udzielenia pomocy właściwym organom publicznym przy rozpatrywaniu wniosków o udzielenie azylu, o wydanie wizy i dokumentów pobytowych oraz związanych z nimi skarg w odniesieniu do celu, jakim jest ustalenie kwalifikowalności osób fizycznych ubiegających się o przyznanie określonego statusu. Systemy sztucznej inteligencji w obszarze zarządzania migracją, azylem i kontrolą graniczną objęte niniejszym rozporządzeniem powinny być zgodne z odpowiednimi wymogami proceduralnymi określonymi w dyrektywie Parlamentu Europejskiego i Rady 2013/32/UE, rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 810/2009 i innych właściwych przepisach.</p>	<p>Systemy sztucznej inteligencji wykorzystywane w zarządzaniu migracją, azylem i kontrolą graniczną mają wpływ na osoby, które często znajdują się w szczególnie trudnej sytuacji i które są zależne od rezultatów działań właściwych organów publicznych. Dokładność, niedyskryminujący charakter i przejrzystość systemów sztucznej inteligencji wykorzystywanych w tych kontekstach są zatem szczególnie istotne w celu zapewnienia poszanowania praw podstawowych zainteresowanych osób, w szczególności ich prawa do swobodnego przemieszczania się, niedyskryminacji, ochrony życia prywatnego i danych osobowych, ochrony międzynarodowej i dobrej administracji. Za systemy wysokiego ryzyka <b>trzeba</b> zatem <b>koniecznie</b> uznać systemy sztucznej inteligencji przeznaczone do wykorzystywania przez właściwe organy publiczne odpowiedzialne za wykonywanie zadań w dziedzinach zarządzania migracją, azylem i kontrolą graniczną jako poligrafy i podobne narzędzia lub do wykrywania stanu emocjonalnego osoby fizycznej; w celu oceny niektórych zagrożeń stwarzanych przez osoby fizyczne wjeżdżające na terytorium państwa członkowskiego lub ubiegające się o wizę lub azyl; w celu weryfikacji autentyczności odpowiednich dokumentów osób fizycznych; w celu udzielenia pomocy właściwym organom publicznym przy rozpatrywaniu wniosków o udzielenie azylu, o wydanie wizy i dokumentów pobytowych oraz związanych z nimi skarg w odniesieniu do celu, jakim jest ustalenie kwalifikowalności osób fizycznych ubiegających się o przyznanie określonego statusu. Systemy sztucznej inteligencji w obszarze zarządzania migracją, azylem i kontrolą graniczną objęte niniejszym rozporządzeniem powinny być zgodne z odpowiednimi wymogami proceduralnymi określonymi w dyrektywie Parlamentu Europejskiego i Rady 2013/32/UE, rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 810/2009 i innych właściwych przepisach.</p>

**Uzasadnienie**

Dostosowanie to odzwierciedla konieczność poddania systemów AI, których dotyczy wnioszek, wzmocnionemu nadzorowi dotyczącemu systemów AI wysokiego ryzyka.

**Poprawka 6**

Motyw 43

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Systemy sztucznej inteligencji wysokiego ryzyka powinny podlegać wymogom dotyczącym jakości wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji użytkownikom, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa. Wymogi te są konieczne, aby skutecznie ograniczyć zagrożenia dla zdrowia, bezpieczeństwa i praw podstawowych, w stosownych przypadkach w świetle przeznaczenia systemu, gdy nie są racjonalnie dostępne inne środki, które powodowałyby mniejsze ograniczenia w handlu, co pozwala uniknąć nieuzasadnionych ograniczeń w handlu.</p>	<p>Systemy sztucznej inteligencji wysokiego ryzyka powinny podlegać wymogom dotyczącym jakości wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji użytkownikom, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa. Wymogi te są konieczne, aby skutecznie ograniczyć zagrożenia dla zdrowia, bezpieczeństwa, <b>bezpieczeństwa danych, praw konsumentów</b> i praw podstawowych, w stosownych przypadkach w świetle przeznaczenia systemu, gdy nie są racjonalnie dostępne inne środki, które powodowałyby mniejsze ograniczenia w handlu, co pozwala uniknąć nieuzasadnionych ograniczeń w handlu. <b>Osoby fizyczne lub grupy osób, których dotyczą systemy sztucznej inteligencji wysokiego ryzyka wprowadzane do obrotu w Unii lub oddane do użytku w inny sposób, powinny być informowane w odpowiedni, łatwo przystępny i zrozumiały sposób oraz móc dotrzeć do jasnych, łatwo dostępnych i publicznych informacji o tym, że podlegają takim systemom.</b></p>

**Uzasadnienie**

Wymogi w zakresie przejrzystości i informacji mające zastosowanie do dostawców i użytkowników należy rozszerzyć na osoby lub grupy osób potencjalnie dotknięte stosowaniem systemów sztucznej inteligencji wysokiego ryzyka, wymienionych w załączniku III do rozporządzenia. „Zrozumiały sposób” oznacza to również język zrozumiały i dostępny dla użytkownika, w tym język mówiony i język migowy.

**Poprawka 7**

Nowy motyw po motywie 44

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
	<p><b>Dostawcy systemów sztucznej inteligencji powstrzymują się od stosowania w swoich systemach zarządzania jakością środków, które promują nieuzasadnioną dyskryminację ze względu na płeć, pochodzenie, religię lub przekonania, niepełnosprawność, wiek, orientację seksualną lub jakiegokolwiek inne przyczyny.</b></p>

**Uzasadnienie**

Bezprawna dyskryminacja ma swoje źródło w działalności człowieka. Dostawcy systemów AI powinni powstrzymać się od stosowania w swoim systemie jakości środków, które mogłyby sprzyjać dyskryminacji.

**Poprawka 8**

Motyw 47

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Aby zapobiec efektowi czarnej skrzynki, który może sprawić, że niektóre systemy sztucznej inteligencji staną się niezrozumiałe lub zbyt skomplikowane dla osób fizycznych, od systemów sztucznej inteligencji wysokiego ryzyka należy wymagać zapewnienia <b>określonego</b> stopnia przejrzystości. Użytkownicy powinni być w stanie interpretować wyniki działania systemu i odpowiednio z nich korzystać. W związku z tym do systemów sztucznej inteligencji wysokiego ryzyka należy dołączać odpowiednią dokumentację i instrukcję obsługi, a w stosownych przypadkach systemy te powinny zawierać zwięzłe i jasne informacje, w tym informacje dotyczące ewentualnego zagrożenia dla praw podstawowych oraz dyskryminacji.</p>	<p>Aby zapobiec efektowi czarnej skrzynki, który może sprawić, że niektóre systemy sztucznej inteligencji staną się niezrozumiałe lub zbyt skomplikowane dla osób fizycznych <b>lub organów publicznych na wszystkich szczeblach sprawowania rządów</b>, od systemów sztucznej inteligencji wysokiego ryzyka należy wymagać zapewnienia <b>wysokiego</b> stopnia przejrzystości. Użytkownicy powinni być w stanie interpretować wyniki działania systemu i odpowiednio z nich korzystać. W związku z tym do systemów sztucznej inteligencji wysokiego ryzyka należy dołączać odpowiednią dokumentację i instrukcję obsługi, a w stosownych przypadkach systemy te powinny zawierać zwięzłe i jasne informacje, w tym informacje dotyczące ewentualnego zagrożenia dla praw podstawowych oraz dyskryminacji.</p>

**Uzasadnienie**

Odpowiedzialność podmiotów, które opracowują systemy AI wysokiego ryzyka, jest osłabiona przez użycie słów „określony stopień przejrzystości”.

**Poprawka 9**

Motyw 48

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Systemy sztucznej inteligencji wysokiego ryzyka należy projektować i opracowywać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie. W tym celu przed wprowadzeniem systemu do obrotu lub jego oddaniem do użytku dostawca systemu powinien określić odpowiednie środki związane z nadzorem ze strony człowieka. W szczególności, w stosownych przypadkach, takie środki powinny gwarantować, że system podlega wbudowanym ograniczeniom operacyjnym, których sam nie jest w stanie obejść, i reaguje na działania człowieka–operatora systemu, oraz że osoby fizyczne, którym powierzono sprawowanie nadzoru ze strony człowieka, posiadają niezbędne kompetencje, przeszkolenie i uprawnienia do pełnienia tej funkcji.</p>	<p>Systemy sztucznej inteligencji wysokiego ryzyka należy projektować i opracowywać w taki sposób, aby osoby fizyczne <b>i organy publiczne na wszystkich szczeblach sprawowania rządów</b> mogły nadzorować ich funkcjonowanie. W tym celu przed wprowadzeniem systemu do obrotu lub jego oddaniem do użytku dostawca systemu powinien określić odpowiednie środki związane z nadzorem ze strony człowieka. W szczególności, w stosownych przypadkach, takie środki powinny gwarantować, że system podlega wbudowanym ograniczeniom operacyjnym, których sam nie jest w stanie obejść, i reaguje na działania człowieka–operatora systemu, oraz że osoby fizyczne, którym powierzono sprawowanie nadzoru ze strony człowieka, posiadają niezbędne kompetencje, przeszkolenie i uprawnienia do pełnienia tej funkcji.</p>

**Uzasadnienie**

Nie wymaga uzasadnienia.

## Poprawka 10

Motyw 67

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Systemy sztucznej inteligencji wysokiego ryzyka powinny posiadać oznakowanie CE świadczące o ich zgodności z niniejszym rozporządzeniem, aby umożliwić ich swobodny przepływ na rynku wewnętrznym. Państwa członkowskie nie powinny stwarzać <b>nieuzasadnionych</b> przeszkód dla wprowadzania do obrotu lub oddawania do użytku systemów sztucznej inteligencji wysokiego ryzyka zgodnych z wymogami określonymi w niniejszym rozporządzeniu i posiadających oznakowanie CE.</p>	<p>Systemy sztucznej inteligencji wysokiego ryzyka powinny posiadać oznakowanie CE świadczące o ich zgodności z niniejszym rozporządzeniem, aby umożliwić ich swobodny przepływ na rynku wewnętrznym. Państwa członkowskie nie powinny stwarzać przeszkód dla wprowadzania do obrotu lub oddawania do użytku systemów sztucznej inteligencji wysokiego ryzyka zgodnych z wymogami określonymi w niniejszym rozporządzeniu i posiadających oznakowanie CE. <b>Państwa członkowskie są uprawnione do regulowania praktyk i systemów sztucznej inteligencji wysokiego ryzyka wyłącznie na podstawie nadrzędnych i należyście uzasadnionych względów bezpieczeństwa narodowego i publicznego.</b></p>

## Uzasadnienie

Chociaż państwa członkowskie nie powinny utrudniać stosowania rozporządzenia, powinny zachować prawo do regulowania systemów sztucznej inteligencji wysokiego ryzyka, jeżeli zagrożone są interesy bezpieczeństwa publicznego i narodowego.

## Poprawka 11

Motyw 70

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Niektóre systemy sztucznej inteligencji przeznaczone do wchodzenia w interakcję z osobami fizycznymi lub tworzenia treści mogą stwarzać szczególne ryzyko podawania się za inną osobę lub świadomego wprowadzania w błąd, niezależnie od tego, czy kwalifikują się jako systemy wysokiego ryzyka, czy też nie. <b>W pewnych okolicznościach</b> korzystanie z tych systemów powinno zatem podlegać szczególnym obowiązkom w zakresie przejrzystości bez uszczerbku dla wymogów i obowiązków określonych dla systemów sztucznej inteligencji wysokiego ryzyka. Osoby fizyczne powinno się w szczególności informować, że prowadzą interakcję z systemem sztucznej inteligencji, <b>chyba że okoliczności i kontekst korzystania z systemu jednoznacznie na to wskazują.</b> Osoby fizyczne należy ponadto informować, gdy mają kontakt z systemem rozpoznawania emocji lub systemem kategoryzacji biometrycznej. Tego rodzaju informacje i powiadomienia należy przekazywać w formatach dostępnych dla osób z niepełnosprawnościami. Ponadto użytkownicy, którzy wykorzystują system sztucznej inteligencji do generowania obrazów, treści dźwiękowych lub treści wideo lub do manipulowania nimi w sposób sprawiający, że zaczynają one budzić przypominać istniejące osoby, miejsca lub zdarzenia, przez co dana osoba mogłaby niesłusznie uznać je za autentyczne, powinny ujawnić, że dane treści zostały sztucznie stworzone lub zmanipulowane poprzez odpowiednie oznakowanie wyniku działania sztucznej inteligencji i ujawnienie, że źródłem danych treści jest system sztucznej inteligencji.</p>	<p>Niektóre systemy sztucznej inteligencji przeznaczone do wchodzenia w interakcję z osobami fizycznymi lub tworzenia treści mogą stwarzać szczególne ryzyko podawania się za inną osobę lub świadomego wprowadzania w błąd, niezależnie od tego, czy kwalifikują się jako systemy wysokiego ryzyka, czy też nie. <b>Korzystanie z tych systemów powinno zatem podlegać szczególnym obowiązkom w zakresie przejrzystości bez uszczerbku dla wymogów i obowiązków określonych dla systemów sztucznej inteligencji wysokiego ryzyka.</b> Osoby fizyczne powinno się w szczególności informować <b>w sposób systematyczny</b>, że prowadzą interakcję z systemem sztucznej inteligencji. Osoby fizyczne należy ponadto informować, gdy mają kontakt z systemem rozpoznawania emocji lub systemem kategoryzacji biometrycznej. Tego rodzaju informacje i powiadomienia należy przekazywać w formatach dostępnych dla osób z niepełnosprawnościami. Ponadto użytkownicy, którzy wykorzystują system sztucznej inteligencji do generowania obrazów, treści dźwiękowych lub treści wideo lub do manipulowania nimi w sposób sprawiający, że zaczynają one budzić przypominać istniejące osoby, miejsca lub zdarzenia, przez co dana osoba mogłaby niesłusznie uznać je za autentyczne, powinny ujawnić, że dane treści zostały sztucznie stworzone lub zmanipulowane poprzez odpowiednie oznakowanie wyniku działania sztucznej inteligencji i ujawnienie, że źródłem danych treści jest system sztucznej inteligencji.</p>

## Uzasadnienie

Nie powinno być żadnych wyjątków od obowiązku przejrzystości i informowania w przypadku interakcji osób fizycznych z systemami AI.

**Poprawka 12**

Motyw 76

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Aby ułatwić sprawne, skuteczne i zharmonizowane wdrożenie niniejszego rozporządzenia, należy ustanowić Europejską Radę ds. Sztucznej Inteligencji. Rada powinna odpowiadać za szereg zadań doradczych, w tym wydawanie opinii lub zaleceń oraz udzielanie porad lub wskazówek w dziedzinach związanych z wdrażaniem niniejszego rozporządzenia, także w sprawie specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w niniejszym rozporządzeniu, jak również za udzielanie porad i wsparcia Komisji w konkretnych kwestiach związanych ze sztuczną inteligencją.</p>	<p>Aby ułatwić sprawne, skuteczne i zharmonizowane wdrożenie niniejszego rozporządzenia, należy ustanowić Europejską Radę ds. Sztucznej Inteligencji. Rada powinna odpowiadać za szereg zadań doradczych, w tym wydawanie opinii lub zaleceń oraz udzielanie porad lub wskazówek w dziedzinach związanych z wdrażaniem niniejszego rozporządzenia, także w sprawie specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w niniejszym rozporządzeniu, jak również za udzielanie porad i wsparcia Komisji w konkretnych kwestiach związanych ze sztuczną inteligencją. <b>Członkowie Europejskiej Rady ds. Sztucznej Inteligencji powinni reprezentować interesy społeczeństwa europejskiego. Skład Europejskiej Rady ds. Sztucznej Inteligencji powinien być zrównoważony pod względem płci.</b></p>

**Uzasadnienie**

Europejska Rada ds. Sztucznej Inteligencji powinna być dobrym odzwierciedleniem szerokich interesów społeczeństwa europejskiego. Obejmują one interesy związane z prawami człowieka, klimatem i energooszczędnym zastosowaniem systemów sztucznej inteligencji, bezpieczeństwem, włączeniem społecznym, zdrowiem itp. Równowaga płci jest warunkiem wstępnym różnorodności w doradztwie, opracowywaniu wytycznych itp.

**Poprawka 13**

Motyw 77

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Państwa członkowskie odgrywają kluczową rolę w stosowaniu i egzekwowaniu niniejszego rozporządzenia. W tym zakresie każde państwo członkowskie powinno wyznaczyć co najmniej jeden właściwy organ krajowy do celów sprawowania nadzoru nad stosowaniem i wdrażaniem niniejszego rozporządzenia. Aby zwiększyć efektywność organizacyjną po stronie państw członkowskich oraz ustanowić oficjalny punkt kontaktowy dla społeczeństwa oraz innych partnerów na szczeblu państw członkowskich i na szczeblu unijnym, w każdym państwie członkowskim należy wyznaczyć jeden organ krajowy jako krajowy organ nadzorczy.</p>	<p>Państwa członkowskie odgrywają kluczową rolę w stosowaniu i egzekwowaniu niniejszego rozporządzenia. W tym zakresie każde państwo członkowskie powinno wyznaczyć co najmniej jeden właściwy organ krajowy do celów sprawowania nadzoru nad stosowaniem i wdrażaniem niniejszego rozporządzenia. Aby zwiększyć efektywność organizacyjną po stronie państw członkowskich oraz ustanowić oficjalny punkt kontaktowy dla społeczeństwa oraz innych partnerów na szczeblu państw członkowskich i na szczeblu unijnym, w każdym państwie członkowskim należy wyznaczyć jeden organ krajowy jako krajowy organ nadzorczy. <b>Władzom lokalnym i regionalnym powierza się zadania w zakresie nadzoru lub egzekwowania przepisów, jeśli państwo członkowskie uzna to za stosowne.</b></p>

**Uzasadnienie**

Aby zapewnić wykonalność rozporządzenia oraz jego ram nadzoru lub egzekwowania przepisów, państwo członkowskie powinno być uprawnione do powierzenia, w stosownych przypadkach i w miarę możliwości, władzom lokalnym i regionalnym zadań związanych z nadzorem lub egzekwowaniem przepisów.

**Poprawka 14**

Motyw 79

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Aby zapewnić odpowiednie i skuteczne egzekwowanie wymogów i obowiązków ustanowionych w niniejszym rozporządzeniu, które należy do unijnego prawodawstwa harmonizacyjnego, system nadzoru rynku i zgodności produktów ustanowiony rozporządzeniem (UE) 2019/1020 powinien mieć zastosowanie w całości. Jeżeli jest to niezbędne do wykonywania ich uprawnień, krajowe organy publiczne lub podmioty prawa publicznego, które nadzorują stosowanie prawa Unii chroniącego prawa podstawowe, w tym organy ds. równości, powinny również mieć dostęp do wszelkiej dokumentacji sporządzonej na podstawie niniejszego rozporządzenia.</p>	<p>Aby zapewnić odpowiednie i skuteczne egzekwowanie wymogów i obowiązków ustanowionych w niniejszym rozporządzeniu, które należy do unijnego prawodawstwa harmonizacyjnego, system nadzoru rynku i zgodności produktów ustanowiony rozporządzeniem (UE) 2019/1020 powinien mieć zastosowanie w całości. Jeżeli jest to niezbędne do wykonywania ich uprawnień, krajowe <b>oraz, w stosownych przypadkach, lokalne lub regionalne</b> organy publiczne lub podmioty prawa publicznego, które nadzorują stosowanie prawa Unii chroniącego prawa podstawowe, w tym organy ds. równości, powinny również mieć dostęp do wszelkiej dokumentacji sporządzonej na podstawie niniejszego rozporządzenia.</p>

**Uzasadnienie**

Niniejsza poprawka uwzględnia różne struktury zarządzania w państwach członkowskich UE.

**Poprawka 15**

Motyw 83

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>W celu zapewnienia opartej na zaufaniu i konstruktywnej współpracy właściwych organów na szczeblu unijnym i krajowym wymagają odpowiedniego wszystkie strony zaangażowane w stosowanie niniejszego rozporządzenia powinny przestrzegać zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań.</p>	<p>W celu zapewnienia opartej na zaufaniu i konstruktywnej współpracy właściwych organów na szczeblu unijnym, krajowym, <b>regionalnym i lokalnym</b> wymagają odpowiedniego wszystkie strony zaangażowane w stosowanie niniejszego rozporządzenia powinny przestrzegać zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań.</p>

**Uzasadnienie**

Niniejsza poprawka uwzględnia różne struktury zarządzania w państwach członkowskich UE.

**Poprawka 16**

Tytuł I art. 3 pkt 1 – Definicje

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>„system sztucznej inteligencji” oznacza <b>oprogramowanie opracowane</b> przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, <b>które</b> może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję;</p>	<p>„system sztucznej inteligencji” oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych <b>w sposób niewyczerpujący</b> w załączniku I, <b>powiązane z praktykami społecznymi, tożsamością i kulturą, które</b> może, dla danego zestawu celów określonych przez człowieka – <b>wychodząc od postrzegania swojego otoczenia poprzez gromadzenie danych, interpretację zebranych ustrukturyzowanych lub nieustrukturyzowanych danych, zarządzanie wiedzą lub przetwarzanie informacji pochodzących z tych danych</b> – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję;</p>

**Uzasadnienie**

System AI składa się z elementów technicznych łączących dane, algorytmy i moc obliczeniową z praktykami społecznymi, społeczeństwem, tożsamością i kulturą. Definicja takiego połączenia elementów społecznych i technicznych nie może zatem ulegać dezaktualizacji i powinna być regularnie aktualizowana w celu dokładnego odzwierciedlenia stale rosnącego wpływu społecznego AI oraz wskazania szybko zmieniających się wyzwań i szans związanych z AI, w tym związku między zarządzaniem wiedzą a sztuczną inteligencją. W tym kontekście algorytmy opracowane przez inne algorytmy również powinny podlegać temu rozporządzeniu.

**Poprawka 17**

Artykuł 5 ust. 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Zakazuje się następujących praktyk w zakresie sztucznej inteligencji:</p> <p>a) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który stosuje techniki podprogowe będące poza świadomością danej osoby w celu istotnego zniekształcenia zachowania tej osoby w sposób, który powoduje lub może powodować u niej lub u innej osoby szkodę fizyczną lub psychiczną;</p> <p>b) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który wykorzystuje dowolne słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne w celu istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób, który powoduje lub może powodować u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną;</p>	<p>Zakazuje się następujących praktyk w zakresie sztucznej inteligencji:</p> <p>a) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który stosuje techniki podprogowe będące poza świadomością danej osoby w sposób, który powoduje lub może powodować u niej lub u innej osoby szkodę fizyczną lub psychiczną, <b><i>narusza lub może naruszać prawa podstawowe innej osoby lub grupy osób, w tym ich fizyczne lub psychiczne zdrowie i bezpieczeństwo, powoduje lub może powodować szkody lub krzywdy dla konsumentów, takie jak straty pieniężne lub dyskryminacja ekonomiczna, lub podważa lub może podważać demokrację i praworządność;</i></b></p> <p>b) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który wykorzystuje dowolne słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne w celu istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób, który powoduje lub może powodować u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną;</p>

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>c) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów sztucznej inteligencji przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości, <b>kiedy to punktowa ocena społeczna prowadzi do jednego lub obu z następujących skutków:</b></p> <p>(i) <b>krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup w kontekstach społecznych, które nie są związane z kontekstami, w których pierwotnie wygenerowano lub zgromadzono dane;</b></p> <p>(ii) <b>krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup, które jest nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi;</b></p> <p>d) wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa, chyba że i w zakresie, w jakim takie wykorzystanie jest absolutnie niezbędne do jednego z następujących celów:</p> <p>(i) ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci;</p> <p>(ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu;</p> <p>(iii) wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa, o którym mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW<sup>(62)</sup> i które w danym państwie członkowskim podlega karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata, zgodnie z prawem danego państwa członkowskiego.</p> <p><sup>(62)</sup> Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002, s. 1).</p>	<p>c) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów sztucznej inteligencji przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych <b>lub grup osób</b> prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości, <b>czego skutkiem jest stosowanie – do celów ogólnych – opartych na sztucznej inteligencji systemów punktowej oceny zachowań społecznych;</b></p> <p>d) <b>wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów sztucznej inteligencji przez organy publiczne lub w ich imieniu, stosowania – do określonych celów – opartych na sztucznej inteligencji systemów punktowej oceny zachowań społecznych bez nadzoru człowieka, tj. w kontekstach społecznych związanych z kontekstami, w których pierwotnie wygenerowano lub zgromadzono dane, na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych lub grup osób prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości, która to punktowa ocena powoduje krzywdzące lub niekorzystne traktowanie niektórych osób fizycznych lub całych ich grup, nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi;</b></p>

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
	<p>e) wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa, chyba że i w zakresie, w jakim takie wykorzystanie jest absolutnie niezbędne do jednego z następujących celów:</p> <ul style="list-style-type: none"> <li>(i) ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci;</li> <li>(ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu;</li> <li>(iii) wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa, o którym mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW <sup>(62)</sup> i które w danym państwie członkowskim podlega karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata, zgodnie z prawem danego państwa członkowskiego.</li> </ul> <p><sup>(62)</sup> Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002, s. 1).</p>

### Uzasadnienie

Ogólnie rzecz biorąc, techniki podprogowe mogą zagrażać wolności, prawom człowieka, a tym samym funkcjonowaniu demokratycznego państwa prawa. Jednocześnie sztuczna inteligencja może naruszać prawa konsumentów. Proponowane uzupełnienia mają na celu wyjaśnienie tej kwestii.

Jeśli chodzi o klasyfikację społeczną przeprowadzaną przez władze publiczne lub w ich imieniu, powinna być ona zakazana, jeżeli jest stosowana w celach ogólnych, biorąc pod uwagę zagrożenia wynikające z takich praktyk, co wyjaśniono w motywie 17. Generowanie lub gromadzenie danych do określonych celów powinno być dozwolone wyłącznie pod nadzorem człowieka i pod warunkiem, że nie narusza to prawa do godności i niedyskryminacji ani nie podważa wartości równości i sprawiedliwości.

**Poprawka 18**

Artykuł 5 ust. 4

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Państwo członkowskie może podjąć decyzję o wprowadzeniu możliwości pełnego lub częściowego zezwolenia na wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa w granicach i na warunkach wymienionych w ust. 1 lit. d), ust. 2 i 3. Dane państwo członkowskie ustanawia w swoim prawie krajowym niezbędne szczegółowe przepisy regulujące wnioski o zezwolenia, o których mowa w ust. 3, wydawanie i wykonywanie tych zezwoleń oraz ich nadzorowanie. W przepisach tych określa się również, w odniesieniu do których celów wymienionych w ust. 1 lit. d), w tym w odniesieniu do których przestępstw, o których mowa w ust. 1 lit. d) ppkt (iii), właściwe organy mogą uzyskać zezwolenie na wykorzystanie powyższych systemów do celów egzekwowania prawa.</p>	<p>Państwo członkowskie może podjąć decyzję o wprowadzeniu możliwości pełnego lub częściowego zezwolenia na wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa w granicach i na warunkach wymienionych w ust. 1 lit. d), ust. 2 i 3. Dane państwo członkowskie ustanawia w swoim prawie krajowym niezbędne szczegółowe przepisy regulujące wnioski o zezwolenia, o których mowa w ust. 3, wydawanie i wykonywanie tych zezwoleń oraz ich nadzorowanie. W przepisach tych określa się również, w odniesieniu do których celów wymienionych w ust. 1 lit. d), w tym w odniesieniu do których przestępstw, o których mowa w ust. 1 lit. d) ppkt (iii), właściwe organy mogą uzyskać zezwolenie na wykorzystanie powyższych systemów do celów egzekwowania prawa. <b>Przepisy te określają zasady informowania zainteresowanych władz lokalnych i regionalnych oraz konsultowania się z nimi. Konsultacje te powinny mieć miejsce przed wyjątkowym wykorzystaniem tych systemów w przestrzeni publicznej. W nagłych sytuacjach, w których nie można racjonalnie oczekiwać uprzednich konsultacji, właściwy organ lokalny i regionalny jest niezwłocznie informowany o wdrożeniu odpowiedniej praktyki z wykorzystaniem sztucznej inteligencji.</b></p>

**Uzasadnienie**

Polityczno-administracyjna odpowiedzialność za zarządzanie przestrzenią publiczną i kontrolę nad nią spoczywa na władzach lokalnych i regionalnych. Powinny one zatem mieć możliwość wniesienia wkładu przed wdrożeniem takich praktyk wykorzystujących AI i być odpowiednio informowane o wyjątkowym wykorzystaniu systemów AI do celów egzekwowania prawa.

W nagłej sytuacji, w której nie można racjonalnie oczekiwać uprzednich konsultacji, niezwłocznie informuje się właściwy organ lokalny lub regionalny.

**Poprawka 19**

Artykuł 13

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Artykuł <b>13</b> Przejrzystość i udostępnianie informacji użytkownikom</p> <p>1. Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w sposób zapewniający wystarczającą przejrzystość ich działania, umożliwiającą użytkownikom interpretację wyników działania systemu i ich właściwe wykorzystanie. Zapewnia się odpowiedni rodzaj i stopień przejrzystości w celu osiągnięcia zgodności z odpowiednimi obowiązkami użytkownika i dostawcy, określonymi w rozdziale 3 niniejszego tytułu.</p>	<p>Artykuł <b>13a</b> Przejrzystość i udostępnianie informacji użytkownikom</p> <p>1. Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w sposób zapewniający wystarczającą przejrzystość ich działania, umożliwiającą użytkownikom interpretację wyników działania systemu i ich właściwe wykorzystanie. Zapewnia się odpowiedni rodzaj i stopień przejrzystości <b>oraz zrozumiałych wyjaśnień</b> w celu osiągnięcia zgodności z odpowiednimi obowiązkami użytkownika i dostawcy, określonymi w rozdziale 3 niniejszego tytułu. <b>Wyjaśnienia są udzielane co najmniej w języku kraju, w którym system sztucznej inteligencji jest wdrażany.</b></p>

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>2. Do systemów sztucznej inteligencji wysokiego ryzyka dołącza się instrukcję obsługi w odpowiednim formacie cyfrowym lub innym formacie zawierającą zwięzłe, kompletne, poprawne i jasne informacje, które są istotne, dostępne i zrozumiałe dla użytkowników.</p> <p>3. Informacje, o których mowa w ust. 2, muszą obejmować:</p> <p>a) tożsamość i dane kontaktowe dostawcy oraz, w stosownych przypadkach, jego upoważnionego przedstawiciela;</p> <p>b) cechy, możliwości i ograniczenia skuteczności działania systemu sztucznej inteligencji wysokiego ryzyka, w tym:</p> <p>(i) jego przeznaczenie;</p> <p>(ii) poziom dokładności, solidności i cyberbezpieczeństwa, o którym mowa w art. 15, względem którego przetestowano system sztucznej inteligencji wysokiego ryzyka i dokonano jego walidacji oraz którego można oczekiwać, a także wszelkie znane i dające się przewidzieć okoliczności, które mogą mieć wpływ na ten oczekiwany poziom dokładności, solidności i cyberbezpieczeństwa;</p> <p>(iii) wszelkie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem systemu sztucznej inteligencji wysokiego ryzyka zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, które mogą powodować zagrożenia dla zdrowia i bezpieczeństwa lub praw podstawowych;</p> <p>(iv) skuteczność działania systemu w odniesieniu do osób lub grup osób, względem których system ma być wykorzystywany;</p> <p>(v) w stosownych przypadkach, specyfikacje dotyczące danych wejściowych lub wszelkie inne istotne informacje dotyczące wykorzystywanych zbiorów danych treningowych, walidacyjnych i testowych, uwzględniając przeznaczenie systemu sztucznej inteligencji;</p>	<p>2. Do systemów sztucznej inteligencji wysokiego ryzyka dołącza się <b>ogólnodostępną, zrozumiałą</b> instrukcję obsługi w odpowiednim formacie cyfrowym lub innym formacie zawierającą zwięzłe, kompletne, poprawne i jasne informacje, które są istotne, dostępne i zrozumiałe dla użytkowników.</p> <p>3. Informacje, o których mowa w ust. 2, muszą obejmować:</p> <p>a) tożsamość i dane kontaktowe dostawcy oraz, w stosownych przypadkach, jego upoważnionego przedstawiciela;</p> <p>b) cechy, możliwości i ograniczenia skuteczności działania systemu sztucznej inteligencji wysokiego ryzyka, w tym:</p> <p>(i) jego przeznaczenie;</p> <p>(ii) poziom dokładności (<b>wyrażony w odpowiedniej metryce do oceny modeli</b>), solidności i cyberbezpieczeństwa, o którym mowa w art. 15, względem którego przetestowano system sztucznej inteligencji wysokiego ryzyka i dokonano jego walidacji oraz którego można oczekiwać, a także wszelkie znane i dające się przewidzieć okoliczności, które mogą mieć wpływ na ten oczekiwany poziom dokładności, solidności i cyberbezpieczeństwa;</p> <p>(iii) wszelkie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem systemu sztucznej inteligencji wysokiego ryzyka zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, które mogą powodować zagrożenia dla zdrowia i bezpieczeństwa lub praw podstawowych;</p> <p>(iv) skuteczność działania systemu w odniesieniu do osób lub grup osób, względem których system ma być wykorzystywany;</p> <p>(v) w stosownych przypadkach, specyfikacje dotyczące danych wejściowych lub wszelkie inne istotne informacje dotyczące wykorzystywanych zbiorów danych treningowych, walidacyjnych i testowych, uwzględniając przeznaczenie systemu sztucznej inteligencji;</p> <p>(vi) <b>parametry za pomocą których model został dostosowany, oraz środki podjęte w celu uniknięcia przetrenowania lub niedostatecznego dopasowania;</b></p>

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>c) ewentualne zmiany w systemie sztucznej inteligencji wysokiego ryzyka i jego skuteczności działania, które zostały z góry zaplanowane przez dostawcę w momencie przeprowadzania pierwotnej oceny zgodności;</p> <p>d) środki nadzoru ze strony człowieka, o których mowa w art. 14, w tym środki techniczne wprowadzone w celu ułatwienia użytkownikom interpretacji wyników działania systemów sztucznej inteligencji;</p> <p>e) przewidywany cykl życia systemu sztucznej inteligencji wysokiego ryzyka oraz wszelkie niezbędne środki w zakresie konserwacji i utrzymania mające na celu zapewnienie właściwego funkcjonowania tego systemu sztucznej inteligencji, w tym dotyczące aktualizacji oprogramowania.</p>	<p>c) ewentualne zmiany w systemie sztucznej inteligencji wysokiego ryzyka i jego skuteczności działania, które zostały z góry zaplanowane przez dostawcę w momencie przeprowadzania pierwotnej oceny zgodności;</p> <p>d) środki nadzoru ze strony człowieka, o których mowa w art. 14, w tym środki techniczne wprowadzone w celu ułatwienia użytkownikom interpretacji wyników działania systemów sztucznej inteligencji;</p> <p>e) przewidywany cykl życia systemu sztucznej inteligencji wysokiego ryzyka oraz wszelkie niezbędne środki w zakresie konserwacji i utrzymania mające na celu zapewnienie właściwego funkcjonowania tego systemu sztucznej inteligencji, w tym dotyczące aktualizacji oprogramowania.</p> <p><b>Artykuł 13b Przejrzystość i informowanie zainteresowanych osób</b></p> <p><i>Osoby lub grupy osób, w przypadku których ma zostać wykorzystany system sztucznej inteligencji wysokiego ryzyka, są informowane w odpowiedni, łatwo przystępny i zrozumiały sposób oraz mogą dotrzeć do jasnych, łatwo dostępnych i publicznych informacji o tym, że podlegają takim systemom.</i></p>

### Uzasadnienie

W celu wzmocnienia ekosystemu zaufania należy publicznie udostępnić instrukcje dotyczące korzystania z systemów AI wysokiego ryzyka. Instrukcje te powinny być napisane w języku kraju, w którym wdrażany jest system AI, zrozumiałym dla czytelnika.

W kontekście przejrzystości i wyjaśnialności algorytmów powinna istnieć możliwość wyjaśnienia, według jakich parametrów model został dostosowany i jakie środki podjęto w celu zapobieżenia jego przetrenowaniu lub niedostatecznemu dopasowaniu.

Art. 13b reguluje obowiązek przejrzystości i informowania osób, które wchodzą w interakcję z systemami AI lub na które system AI może mieć wpływ.

### Poprawka 20

Artykuł 14 ust. 4

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Osobom, którym powierzono sprawowanie nadzoru ze strony człowieka, środki, o których mowa w ust. 3, muszą umożliwiać, odpowiednio do okoliczności:</p> <p>a) zrozumienie w pełni możliwości i ograniczeń systemu sztucznej inteligencji wysokiego ryzyka oraz należyte monitorowanie jego działania, tak aby oznaki anomalii, nieprawidłowego funkcjonowania i nieoczekiwanych wyników działania można było wykrywać i zaradzić im tak szybko, jak to możliwe;</p>	<p>Osobom, którym powierzono sprawowanie nadzoru ze strony człowieka, środki, o których mowa w ust. 3, muszą umożliwiać, odpowiednio do okoliczności:</p> <p>a) zrozumienie w pełni możliwości i ograniczeń systemu sztucznej inteligencji wysokiego ryzyka oraz należyte monitorowanie jego działania, tak aby oznaki anomalii, nieprawidłowego funkcjonowania i nieoczekiwanych wyników działania można było wykrywać i zaradzić im tak szybko, jak to możliwe;</p>

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
b) bycie stale świadomym potencjalnej tendencji do automatycznego polegania lub nadmiernego polegania na wyniku działania systemu sztucznej inteligencji wysokiego ryzyka (tzw. „automation bias”), w szczególności w przypadku systemów sztucznej inteligencji wysokiego ryzyka wykorzystywanych do udzielania informacji lub zaleceń na potrzeby decyzji podejmowanych przez osoby fizyczne;	b) bycie stale świadomym potencjalnej tendencji do automatycznego polegania lub nadmiernego polegania na wyniku działania systemu sztucznej inteligencji wysokiego ryzyka (tzw. „automation bias”), <b>lub jakiegokolwiek innej formy stronniczości (tzw. „bias”)</b> , w szczególności w przypadku systemów sztucznej inteligencji wysokiego ryzyka wykorzystywanych do udzielania informacji lub zaleceń na potrzeby decyzji podejmowanych przez osoby fizyczne;
c) prawidłową interpretację wyniku działania systemu sztucznej inteligencji wysokiego ryzyka, biorąc pod uwagę w szczególności cechy systemu oraz dostępne narzędzia i metody interpretacji;	c) prawidłową interpretację wyniku działania systemu sztucznej inteligencji wysokiego ryzyka, biorąc pod uwagę w szczególności cechy systemu oraz dostępne narzędzia i metody interpretacji;
d) podjęcie decyzji, w każdej konkretnej sytuacji, o niekorzystaniu z systemu sztucznej inteligencji wysokiego ryzyka lub w inny sposób zignorowanie, ręczną zmianę lub odwrócenie wyniku działania systemu sztucznej inteligencji wysokiego ryzyka;	d) podjęcie decyzji, w każdej konkretnej sytuacji, o niekorzystaniu z systemu sztucznej inteligencji wysokiego ryzyka lub w inny sposób zignorowanie, ręczną zmianę lub odwrócenie wyniku działania systemu sztucznej inteligencji wysokiego ryzyka;
e) ingerowanie w działanie systemu sztucznej inteligencji wysokiego ryzyka lub przerwanie działania systemu za pomocą przycisku „stop” lub podobnej procedury.	e) ingerowanie w działanie systemu sztucznej inteligencji wysokiego ryzyka lub przerwanie działania systemu za pomocą przycisku „stop” lub podobnej procedury.

### Uzasadnienie

Istnieje kilka form stronniczości, które mogą być problematyczne. Należą do nich: uprzedzenia projektanta lub użytkownika do systemu AI (social bias), uprzedzenia dotyczące tego, czy wdrożony system AI jest odpowiednim rozwiązaniem problemu (techno bias) oraz statystyczne formy stronniczości.

### Poprawka 21

Artykuł 14 – nowy ustęp po ustępie 5

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
	<b><i>Wszelkie decyzje podejmowane przez systemy sztucznej inteligencji, o których mowa w załączniku III pkt 5 lit. a) i b), muszą być uzależnione od interwencji człowieka i oparte na starannym procesie decyzyjnym. Należy zapewnić kontakty międzyludzkie przy podejmowaniu tych decyzji.</i></b>

### Uzasadnienie

Art. 14 dotyczy wyłącznie nadzoru ludzkiego nad systemami sztucznej inteligencji wysokiego ryzyka. W odniesieniu do decyzji podejmowanych przez władze publiczne należy podkreślić, że gwarantuje się interwencję człowieka, kontakt i poszanowanie procedur.

**Poprawka 22**

Artykuł 17 ust. 1, dodać dwie litery po lit. m)

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Dostawcy systemów sztucznej inteligencji wysokiego ryzyka wprowadzają system zarządzania jakością, który zapewnia zgodność z niniejszym rozporządzeniem. System ten dokumentuje się w systematyczny i uporządkowany sposób w formie pisemnych polityk, procedur i instrukcji oraz obejmuje on co najmniej następujące aspekty:</p>	<p>Dostawcy systemów sztucznej inteligencji wysokiego ryzyka wprowadzają system zarządzania jakością, który zapewnia zgodność z niniejszym rozporządzeniem. System ten dokumentuje się w systematyczny i uporządkowany sposób w formie pisemnych polityk, procedur i instrukcji oraz obejmuje on co najmniej następujące aspekty:</p>
<p>a) strategię zgodności regulacyjnej, w tym zgodności z procedurami oceny zgodności i procedurami zarządzania zmianami w systemie sztucznej inteligencji wysokiego ryzyka;</p>	<p>a) strategię zgodności regulacyjnej, w tym zgodności z procedurami oceny zgodności i procedurami zarządzania zmianami w systemie sztucznej inteligencji wysokiego ryzyka;</p>
<p>b) techniki, procedury i systematyczne działania, które należy stosować na potrzeby projektowania oraz kontroli i weryfikacji projektu systemu sztucznej inteligencji wysokiego ryzyka;</p>	<p>b) techniki, procedury i systematyczne działania, które należy stosować na potrzeby projektowania oraz kontroli i weryfikacji projektu systemu sztucznej inteligencji wysokiego ryzyka;</p>
<p>c) techniki, procedury i systematyczne działania, które należy stosować na potrzeby opracowywania, kontroli jakości i zapewniania jakości systemu sztucznej inteligencji wysokiego ryzyka;</p>	<p>c) techniki, procedury i systematyczne działania, które należy stosować na potrzeby opracowywania, kontroli jakości i zapewniania jakości systemu sztucznej inteligencji wysokiego ryzyka;</p>
<p>d) procedury badania, testowania i walidacji, które należy przeprowadzić przed rozpoczęciem opracowywania systemu sztucznej inteligencji wysokiego ryzyka, w trakcie tego procesu i po jego zakończeniu, oraz częstotliwość, z jaką mają być przeprowadzane;</p>	<p>d) procedury badania, testowania i walidacji, które należy przeprowadzić przed rozpoczęciem opracowywania systemu sztucznej inteligencji wysokiego ryzyka, w trakcie tego procesu i po jego zakończeniu, oraz częstotliwość, z jaką mają być przeprowadzane;</p>
<p>e) specyfikacje techniczne, w tym normy, jakie należy stosować, a w przypadku gdy nie stosuje się w pełni odpowiednich norm zharmonizowanych, środki, jakie należy zastosować w celu zapewnienia zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami określonymi w rozdziale 2 niniejszego tytułu;</p>	<p>e) specyfikacje techniczne, w tym normy, jakie należy stosować, a w przypadku gdy nie stosuje się w pełni odpowiednich norm zharmonizowanych, środki, jakie należy zastosować w celu zapewnienia zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami określonymi w rozdziale 2 niniejszego tytułu;</p>
<p>f) systemy i procedury zarządzania danymi, w tym gromadzenia danych, analizy danych, etykietowania danych, przechowywania danych, filtrowania danych, eksploracji danych, agregacji danych, zatrzymywania danych i wszelkich innych operacji dotyczących danych, które przeprowadza się przed wprowadzeniem do obrotu lub oddaniem do użytku systemów sztucznej inteligencji wysokiego ryzyka i do celów wprowadzenia ich do obrotu lub oddania ich do użytku;</p>	<p>f) systemy i procedury zarządzania danymi, w tym gromadzenia danych, analizy danych, etykietowania danych, przechowywania danych, filtrowania danych, eksploracji danych, agregacji danych, zatrzymywania danych i wszelkich innych operacji dotyczących danych, które przeprowadza się przed wprowadzeniem do obrotu lub oddaniem do użytku systemów sztucznej inteligencji wysokiego ryzyka i do celów wprowadzenia ich do obrotu lub oddania ich do użytku;</p>
<p>g) system zarządzania ryzykiem, o którym mowa w art. 9;</p>	<p>g) system zarządzania ryzykiem, o którym mowa w art. 9;</p>
<p>h) ustanowienie, wdrożenie i utrzymanie systemu monitorowania po wprowadzeniu do obrotu, zgodnie z art. 61;</p>	<p>h) ustanowienie, wdrożenie i utrzymanie systemu monitorowania po wprowadzeniu do obrotu, zgodnie z art. 61;</p>

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>i) procedury związane ze zgłaszaniem poważnych incydentów i nieprawidłowego działania zgodnie z art. 62;</p> <p>j) obsługę komunikacji z właściwymi organami krajowymi, właściwymi organami, w tym sektorowymi, zapewniającymi lub wspierającymi dostęp do danych, jednostkami notyfikowanymi, innymi operatorami, klientami lub innymi zainteresowanymi stronami;</p> <p>k) systemy i procedury ewidencjonowania wszelkiej istotnej dokumentacji i wszelkich istotnych informacji;</p> <p>l) zarządzanie zasobami, w tym środki związane z bezpieczeństwem dostaw;</p> <p>m) ramy odpowiedzialności służące określeniu obowiązków kierownictwa i pozostałego personelu w odniesieniu do wszystkich aspektów wymienionych w niniejszym ustępie.</p>	<p>i) procedury związane ze zgłaszaniem poważnych incydentów i nieprawidłowego działania zgodnie z art. 62;</p> <p>j) obsługę komunikacji z właściwymi organami krajowymi, właściwymi organami, w tym sektorowymi, zapewniającymi lub wspierającymi dostęp do danych, jednostkami notyfikowanymi, innymi operatorami, klientami lub innymi zainteresowanymi stronami;</p> <p>k) systemy i procedury ewidencjonowania wszelkiej istotnej dokumentacji i wszelkich istotnych informacji;</p> <p>l) zarządzanie zasobami, w tym środki związane z bezpieczeństwem dostaw;</p> <p>m) ramy odpowiedzialności służące określeniu obowiązków kierownictwa i pozostałego personelu w odniesieniu do wszystkich aspektów wymienionych w niniejszym ustępie;</p> <p><i>n) środki mające na celu zapobieganie nieuzasadnionej dyskryminacji ze względu na płeć, pochodzenie etniczne, religię lub przekonania, niepełnosprawność, wiek, orientację seksualną lub jakiegokolwiek inne przyczyny;</i></p> <p><i>o) wyjaśnienie, w jaki sposób kwestie etyczne zostały uwzględnione przy projektowaniu systemu sztucznej inteligencji wysokiego ryzyka.</i></p>

### Uzasadnienie

W dodanym tekście podkreśla się, że włączenie społeczne i walka z nieuzasadnioną dyskryminacją powinny być ważnymi elementami systemu jakości.

System musi spełniać wartości etyczne, które użytkownik systemu AI chce przypisać temu systemowi lub co do których dostawca może w sposób uzasadniony oczekiwać, że ich spełnienie będzie wymagane od systemu AI wysokiego ryzyka. Dostawca musi być w stanie wyjaśnić, w jaki sposób wziął to pod uwagę.

### Poprawka 23

#### Artykuł 19 ustęp 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Dostawcy systemów sztucznej inteligencji wysokiego ryzyka zapewniają, aby ich systemy poddawano odpowiedniej procedurze oceny zgodności zgodnie z art. 43 przed wprowadzeniem ich do obrotu lub oddaniem ich do użytku. W przypadku wykazania zgodności systemów sztucznej inteligencji z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu w wyniku wspomnianej oceny zgodności dostawcy sporządzają deklarację zgodności UE zgodnie z art. 48 i umieszczają oznakowanie zgodności CE zgodnie z art. 49.</p>	<p>Dostawcy systemów sztucznej inteligencji wysokiego ryzyka zapewniają, aby ich systemy poddawano odpowiedniej procedurze oceny zgodności zgodnie z art. 43 przed wprowadzeniem ich do obrotu lub oddaniem ich do użytku. W przypadku wykazania zgodności systemów sztucznej inteligencji z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu w wyniku wspomnianej oceny zgodności dostawcy sporządzają deklarację zgodności UE zgodnie z art. 48 i umieszczają oznakowanie zgodności CE zgodnie z art. 49. <b>Dostawca systemów sztucznej inteligencji wysokiego ryzyka publikuje deklarację zgodności UE oraz streszczenie oceny zgodności w miejscu publicznie dostępnym.</b></p>

**Uzasadnienie**

W celu wzmocnienia ekosystemu zaufania do systemów AI, dostawcy systemów AI wysokiego ryzyka powinni wykazywać się otwartością. Opinia publiczna powinna zatem mieć możliwość sprawdzenia, czy ocena zgodności została właściwie przeprowadzona zgodnie z przepisami rozporządzenia.

**Poprawka 24**

Artykuł 29 nowy ustęp po ustępie 6

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
	<p><i>Użytkownicy systemów sztucznej inteligencji wysokiego ryzyka są odpowiedzialni za dokonanie oceny etycznej przed wprowadzeniem systemu do obrotu. Są w stanie wyjaśnić ewentualny wpływ wdrożenia technologii na ludzi i społeczeństwo. Określają zamierzony cel wdrożenia systemu sztucznej inteligencji, wartości nadrzędne i sposób wyważenia tych wartości oraz sposób, w jaki wartości te zostały wyważone i wdrożone lub nie do systemu. Oceniają rzeczywisty wpływ systemu na ludzi i społeczeństwo w całym cyklu życia systemu sztucznej inteligencji.</i></p>

**Uzasadnienie**

Etyka jest szerokim pojęciem. Istnieje wiele sposobów stosowania etyki technologicznej, zarówno pod względem teoretycznych uzasadnień, jak i konkretnych metod, narzędzi i wartości projektowych. Wartości są kwestiami uznawanymi za ważne przez niektóre grupy ludzi. Mogą być bardziej konkretne lub bardziej koncepcyjne. Ważne jest utrzymanie otwartego zakresu wartości moralnych, które ewentualnie należało będzie wdrożyć, oraz dalsza ocena cyklu życia systemu AI.

**Poprawka 25**

Artykuł 52 ustęp 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Dostawcy zapewniają, aby systemy sztucznej inteligencji przeznaczone do wchodzenia w interakcję z osobami fizycznymi projektowano i opracowywano w taki sposób, aby osoby fizyczne były informowane o tym, że prowadzą interakcję z systemem sztucznej inteligencji, <b>chyba że okoliczności i kontekst korzystania z systemu jednoznacznie na to wskazują</b>. Obowiązek ten nie ma zastosowania do systemów sztucznej inteligencji zatwierdzonych z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia dochodzeń/śledztw w związku z przestępstwami i ścigania ich sprawców, chyba że systemy te udostępnia się ogółowi społeczeństwa na potrzeby składania zawiadomień o popełnieniu przestępstwa.</p>	<p>Dostawcy zapewniają, aby systemy sztucznej inteligencji przeznaczone do wchodzenia w interakcję z osobami fizycznymi projektowano i opracowywano w taki sposób, aby osoby fizyczne były informowane o tym, że prowadzą interakcję z systemem sztucznej inteligencji. Obowiązek ten nie ma zastosowania do systemów sztucznej inteligencji zatwierdzonych z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia dochodzeń/śledztw w związku z przestępstwami i ścigania ich sprawców, chyba że systemy te udostępnia się ogółowi społeczeństwa na potrzeby składania zawiadomień o popełnieniu przestępstwa. <b>Paleta wyboru i status prawny osób fizycznych prowadzących interakcję z systemami sztucznej inteligencji nie powinny być ograniczone przez tę interakcję.</b></p>

**Uzasadnienie**

W przypadku, gdy artefakty technologiczne są wykorzystywane jako środek interakcji z osobami fizycznymi, może istnieć ryzyko ograniczenia wyborów osób fizycznych wchodzących w interakcję z tymi artefaktami. Osoby fizyczne powinny być zawsze należycie informowane o każdym przypadku interakcji z systemami sztucznej inteligencji i nie powinno to być przedmiotem interpretacji danej sytuacji. Ich prawa powinny być zawsze zagwarantowane w interakcjach z systemami AI.

**Poprawka 26**

## Artykuł 57 ustęp 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>W skład Rady wchodzić krajowe organy nadzorcze reprezentowane przez osobę stojącą na czele danego organu lub równoważnego wysokiego rangą urzędnika danego organu oraz Europejski Inspektor Ochrony Danych. Inne organy krajowe mogą być zapraszane na posiedzenia Rady, na których omawia się istotne dla nich kwestie.</p>	<p>W skład Rady wchodzić krajowe organy nadzorcze reprezentowane przez osobę stojącą na czele danego organu lub równoważnego wysokiego rangą urzędnika danego organu oraz Europejski Inspektor Ochrony Danych. Inne organy krajowe, <b>regionalne i lokalne</b> mogą być zapraszane na posiedzenia Rady, na których omawia się istotne dla nich kwestie.</p>

**Uzasadnienie**

Władze lokalne i regionalne muszą również mieć możliwość udziału w monitorowaniu systemów AI i składania sprawozdań z ich wdrażania w terenie.

**Poprawka 27**

## Artykuł 58

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Udzielając Komisji porad i wsparcia zgodnie z art. 56 ust. 2, Rada w szczególności:</p> <p>a) gromadzi wiedzę fachową i najlepsze praktyki i udostępnia je państwom członkowskim;</p> <p>b) wnosi wkład w wypracowywanie jednolitych praktyk administracyjnych w państwach członkowskich, w tym praktyk w zakresie funkcjonowania piaskownic regulacyjnych, o których mowa w art. 53;</p> <p>c) wydaje opinie, zalecenia lub pisemne uwagi dotyczące kwestii związanych z wdrażaniem niniejszego rozporządzenia, w szczególności:</p> <p>(i) w kwestii specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w tytule III rozdział 2,</p> <p>(ii) w kwestii stosowania norm zharmonizowanych lub wspólnych specyfikacji, o których mowa w art. 40 i 41,</p> <p>(iii) w kwestii sporządzania wytycznych, z uwzględnieniem wytycznych dotyczących ustalania wysokości administracyjnych kar pieniężnych, o których mowa w art. 71.</p>	<p>Udzielając Komisji porad i wsparcia zgodnie z art. 56 ust. 2, Rada w szczególności:</p> <p>a) gromadzi wiedzę fachową i najlepsze praktyki i udostępnia je państwom członkowskim, <b>władzom regionalnym i lokalnym</b>;</p> <p>b) wnosi wkład w wypracowywanie jednolitych praktyk administracyjnych w państwach członkowskich, w tym praktyk w zakresie funkcjonowania piaskownic regulacyjnych, o których mowa w art. 53;</p> <p>c) wydaje opinie, zalecenia lub pisemne uwagi dotyczące kwestii związanych z wdrażaniem niniejszego rozporządzenia, w szczególności:</p> <p>(i) w kwestii specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w tytule III rozdział 2,</p> <p>(ii) w kwestii stosowania norm zharmonizowanych lub wspólnych specyfikacji, o których mowa w art. 40 i 41,</p> <p>(iii) w kwestii sporządzania wytycznych, z uwzględnieniem wytycznych dotyczących ustalania wysokości administracyjnych kar pieniężnych, o których mowa w art. 71.</p>

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
--	---------------

### Uzasadnienie

Władze lokalne i regionalne znajdują się najbliżej lokalnych mieszkańców i gospodarek. Należy im wyraźnie przydzielić dobrą pozycję, jeśli chodzi o dzielenie się wiedzą.

### Poprawka 28

Artykuł 59 ustęp 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Każde państwo członkowskie ustanawia lub wyznacza właściwe organy krajowe na potrzeby zapewnienia stosowania i wdrażania niniejszego rozporządzenia. Właściwe organy krajowe organizuje się w sposób gwarantujący obiektywizm i bezstronność podejmowanych przez nie działań i wykonywanych przez nie zadań.</p>	<p>Każde państwo członkowskie ustanawia lub wyznacza właściwe organy krajowe na potrzeby zapewnienia stosowania i wdrażania niniejszego rozporządzenia. Właściwe organy krajowe organizuje się w sposób gwarantujący obiektywizm i bezstronność podejmowanych przez nie działań i wykonywanych przez nie zadań. <b>Władze lokalne i regionalne są uprawnione do wykonywania zadań w zakresie nadzoru lub egzekwowania przepisów, jeśli państwo członkowskie uzna to za stosowne.</b></p>

### Uzasadnienie

Aby zapewnić wykonalność rozporządzenia oraz określonych ram nadzoru lub egzekwowania przepisów, państwo członkowskie powinno być w stanie powierzyć, w stosownych przypadkach i w miarę możliwości, władzom lokalnym i regionalnym zadania związane z nadzorem lub egzekwowaniem przepisów. W tym kontekście władze lokalne i regionalne muszą otrzymać wsparcie i szkolenia, aby były w pełni uprawnione do wykonywania zadań w zakresie nadzoru lub egzekwowania przepisów.

### Poprawka 29

Artykuł 69 ustęp 3

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Kodeksy postępowania mogą być opracowywane przez poszczególnych dostawców systemów sztucznej inteligencji lub przez reprezentujące ich organizacje bądź przez obie te grupy, w tym z udziałem użytkowników i wszelkich zainteresowanych stron oraz reprezentujących je organizacji. Kodeksy postępowania mogą obejmować jeden lub większą liczbę systemów sztucznej inteligencji, mając na uwadze podobieństwa w przeznaczeniu danych systemów.</p>	<p>Kodeksy postępowania mogą być opracowywane przez <b>władze krajowe, lokalne lub regionalne</b>, poszczególnych dostawców systemów sztucznej inteligencji lub przez reprezentujące ich organizacje bądź przez obie te grupy, w tym z udziałem użytkowników i wszelkich zainteresowanych stron oraz reprezentujących je organizacji. Kodeksy postępowania mogą obejmować jeden lub większą liczbę systemów sztucznej inteligencji, mając na uwadze podobieństwa w przeznaczeniu danych systemów.</p>

### Uzasadnienie

Władzom krajowym, lokalnym i regionalnym należy przyznać uprawnienia do sporządzania kodeksów postępowania dla opracowywanych lub stosowanych przez nie systemów AI.

**Poprawka 30**

ZAŁĄCZNIK I – Techniki i podejścia z zakresu sztucznej inteligencji, o których mowa w art. 3 ust. 1

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>a) mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego;</p> <p>b) metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) i systemy ekspertowe;</p> <p>c) podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji.</p>	<p><b>Biorąc pod uwagę obecny stan nauki, sztuczna inteligencja obejmuje następujące techniki i metody:</b></p> <p>a) mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego;</p> <p>b) metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) i systemy ekspertowe;</p> <p>c) podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji.</p>

**Uzasadnienie**

Definicja i wykaz technik AI nie mogą ulegać dezaktualizacji. Wykaz konkretnych technik i podejść stosowanych do rozwoju systemów AI nie powinien być wyczerpujący i musi być jasne, że opiera się on na aktualnej wiedzy naukowej.

**Poprawka 31**

Załącznik III, pkt 1–5

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>Systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. 6 ust. 2 to systemy sztucznej inteligencji wymienione w którymkolwiek z poniższych obszarów:</p> <p>1. identyfikacja i kategoryzacja biometryczna osób fizycznych:</p> <p>a) systemy sztucznej inteligencji przeznaczone do stosowania w celu zdalnej identyfikacji biometrycznej osób fizycznych „w czasie rzeczywistym” i „post factum”;</p> <p>2. zarządzanie infrastrukturą krytyczną i jej eksploatacja:</p> <p>a) systemy sztucznej inteligencji przeznaczone do stosowania jako związane z bezpieczeństwem elementy procesów zarządzania i obsługi ruchu drogowego oraz zaopatrzenia w wodę, gaz, ciepło i energię elektryczną;</p>	<p>Systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. 6 ust. 2 to systemy sztucznej inteligencji wymienione w którymkolwiek z poniższych obszarów:</p> <p>1. identyfikacja i kategoryzacja biometryczna osób fizycznych:</p> <p>a) systemy sztucznej inteligencji przeznaczone do stosowania w celu zdalnej identyfikacji biometrycznej osób fizycznych „w czasie rzeczywistym” i „post factum”;</p> <p>2. zarządzanie infrastrukturą krytyczną i jej eksploatacja:</p> <p>a) systemy sztucznej inteligencji przeznaczone do stosowania jako związane z bezpieczeństwem elementy procesów zarządzania i obsługi ruchu drogowego oraz zaopatrzenia w wodę, gaz, ciepło i energię elektryczną <b>oraz infrastrukturę telekomunikacyjną, wodociagową i internetową;</b></p>

Tekst zaproponowany przez Komisję Europejską	Poprawka KR-u
<p>3. kształcenie i szkolenie zawodowe:</p> <p>a) systemy sztucznej inteligencji przeznaczone do stosowania w celu podejmowania decyzji o dostępie do instytucji edukacyjnych i instytucji szkolenia zawodowego lub nadawania osobom przydziału do tych instytucji;</p> <p>b) systemy sztucznej inteligencji przeznaczone do stosowania w celu oceny uczniów w instytucjach edukacyjnych i instytucji szkolenia zawodowego oraz do oceny uczestników egzaminów powszechnie wymaganych w celu przyjęcia do instytucji edukacyjnych;</p> <p>4. zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia:</p> <p>a) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu rekrutacji lub wyboru osób fizycznych, w szczególności w przypadku informowania o wakatach, selekcji lub filtrowania podań o pracę, oceny kandydatów w trakcie rozmów kwalifikacyjnych lub testów;</p> <p>b) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu podejmowania decyzji o awansie i rozwiązaniu stosunku pracy, przydzielania zadań oraz monitorowania i oceny wydajności i zachowania osób pozostających w takich stosunkach;</p> <p>5. dostęp do podstawowych usług prywatnych oraz usług i świadczeń publicznych, a także korzystanie z nich:</p> <p>a) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy publiczne lub w imieniu organów publicznych w celu <b>oceny</b> kwalifikowalności osób fizycznych do świadczeń i usług publicznych, jak również w celu przyznawania, ograniczania, unieważniania lub żądania zwrotu takich świadczeń i usług;</p> <p>b) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu <b>oceny</b> zdolności kredytowej osób fizycznych lub <b>ustalenia</b> ich punktowej oceny kredytowej, z wyjątkiem systemów sztucznej inteligencji oddawanych do użytku przez drobnych dostawców na ich własny użytek;</p> <p>c) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu wysyłania lub ustalania priorytetów w wysyłaniu służb ratunkowych w sytuacjach kryzysowych, w tym straży pożarnej i pomocy medycznej;</p>	<p>3. kształcenie i szkolenie zawodowe:</p> <p>a) systemy sztucznej inteligencji przeznaczone do stosowania w celu podejmowania decyzji o dostępie do instytucji edukacyjnych i instytucji szkolenia zawodowego lub nadawania osobom przydziału do tych instytucji;</p> <p>b) systemy sztucznej inteligencji przeznaczone do stosowania w celu oceny uczniów w instytucjach edukacyjnych i instytucji szkolenia zawodowego oraz do oceny uczestników egzaminów powszechnie wymaganych w celu przyjęcia do instytucji edukacyjnych;</p> <p>4. zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia:</p> <p>a) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu rekrutacji lub wyboru osób fizycznych, w szczególności w przypadku informowania o wakatach, selekcji lub filtrowania podań o pracę, oceny kandydatów w trakcie rozmów kwalifikacyjnych lub testów;</p> <p>b) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu podejmowania decyzji o awansie i rozwiązaniu stosunku pracy, przydzielania zadań oraz monitorowania i oceny wydajności i zachowania osób pozostających w takich stosunkach;</p> <p>5. dostęp do podstawowych usług prywatnych oraz usług i świadczeń publicznych, a także korzystanie z nich:</p> <p>a) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy publiczne lub w imieniu organów publicznych w celu <b>oceny</b> kwalifikowalności osób fizycznych do świadczeń i usług publicznych <b>oraz decydowania o niej</b>, jak również w celu przyznawania, ograniczania, unieważniania lub żądania zwrotu takich świadczeń i usług;</p> <p>b) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu <b>ustalenia</b> zdolności kredytowej osób fizycznych lub ich punktowej oceny kredytowej, z wyjątkiem systemów sztucznej inteligencji oddawanych do użytku przez drobnych dostawców na ich własny użytek;</p> <p>c) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu wysyłania lub ustalania priorytetów w wysyłaniu służb ratunkowych w sytuacjach kryzysowych, w tym straży pożarnej i pomocy medycznej;</p>

### Uzasadnienie

Infrastruktura telekomunikacyjna, wodociągowa i internetowa stanowią integralną część infrastruktury krytycznej.

Przy kwalifikacji systemów wysokiego ryzyka istotne jest to, czy systemy takie mogą stanowić rzeczywiste zagrożenie dla obywateli. Sama analityczna i teoretyczna ocena roszczeń mieszkańców wobec usług publicznych nie wiąże się z wysokim ryzykiem. Uzupełnienie słowa „ocena” słowem „decydowanie” podkreśla, że ryzyko to jest skutecznie odzwierciedlone w procesie podejmowania decyzji, w szczególności w odniesieniu do mieszkańców.

## II. ZALECENIA POLITYCZNE

EUROPEJSKI KOMITET REGIONÓW

### Ekosystem doskonałości

1. Podkreśla, że ambicje Komisji, by uczynić UE światowym liderem w zakresie odpowiedzialnego i ukierunkowanego na ludzi rozwoju sztucznej inteligencji, można zrealizować jedynie przy silnej pozycji władz lokalnych i regionalnych. Władze lokalne i regionalne są najlepiej predestynowane do tego, by przyczynić się do stworzenia warunków sprzyjających rozwojowi inwestycji w sztuczną inteligencję w nadchodzących latach oraz do zwiększenia zaufania do sztucznej inteligencji.
2. Podkreśla, że oprócz zaangażowania władz lokalnych i regionalnych ważne jest zapewnienie im wsparcia i szkoleń w celu zwiększenia ich kompetencji w tej dziedzinie, zwłaszcza że mogą one pełnić funkcje związane z nadzorem lub egzekwowaniem przepisów.
3. Zauważa, że finansowanie UE będzie dostępne na rozwój sztucznej inteligencji, ale wskazuje na fragmentaryczne podejście do rozwoju AI ze względu na różnorodność programów, co zwiększa ryzyko fragmentacji i nakładania się działań.
4. W związku z tym wzywa Komisję do opracowania i połączenia silnych i pluralistycznych wspólnych przestrzeni danych, w których społeczne przypadki użycia rozwiązywane są poprzez wykorzystanie danych publicznych i prywatnych. Wymaga to również dostosowania do inicjatyw ustawodawczych w ramach europejskiej strategii w zakresie danych.

### Ekosystem zaufania

5. Wyraża ubolewanie, że we wniosku dotyczącym rozporządzenia nie wspomina się o władzach lokalnych i regionalnych, pomimo że ramy prawne będą miały zastosowanie zarówno do podmiotów publicznych, jak i prywatnych.
6. Zauważa w związku z tym, że systemy AI mogą odgrywać ważną rolę w kontaktach władz lokalnych i regionalnych z obywatelami i w świadczeniu usług. Ponadto mogą, między innymi, poprawić wydajność sektora publicznego i pomóc władzom lokalnym i regionalnym w reagowaniu na dostosowania, które należy przeprowadzić na szczeblu lokalnym i regionalnym w kontekście transformacji ekologicznej i cyfrowej. Ważne jest zatem, aby doświadczenia władz lokalnych i regionalnych były aktywnie wykorzystywane przy trwającym przeglądzie rozporządzenia.
7. Apeluje o dalsze doprecyzowanie definicji „dostawcy” i „użytkownika”, zwłaszcza w sytuacjach, gdy przedsiębiorstwa, instytucje badawcze, władze publiczne i mieszkańcy wspólnie opracowują i testują systemy sztucznej inteligencji w żywych laboratoriach. Trzeba również zwrócić należytą uwagę na obywateli lub konsumentów, których dotyczą decyzje podejmowane w oparciu o AI w systemach stosowanych przez użytkowników profesjonalnych.
8. Podkreśla potrzebę uprzedniej konsultacji z zainteresowanymi władzami lokalnymi i regionalnymi w przypadku wykorzystania systemów sztucznej inteligencji do identyfikacji biometrycznej w czasie rzeczywistym osób fizycznych na odległość w publicznie dostępnej przestrzeni w celu egzekwowania prawa.
9. Z zadowoleniem przyjmuje konsultacje publiczne Komisji Europejskiej w sprawie dostosowania przepisów dotyczących odpowiedzialności cywilnej do szczególnych wyzwań związanych z epoką cyfrową i sztuczną inteligencją<sup>(1)</sup> i oczekuje, że doprowadzi to do aktualizacji ram mających na celu zapewnienie dochodzenia roszczeń przez konsumentów za szkody spowodowane zastosowaniami sztucznej inteligencji.
10. Zastanawia się, dlaczego systemy AI wykorzystywane w procesach demokratycznych, takich jak wybory, nie znajdują się na liście systemów AI wysokiego ryzyka.
11. Apeluje, aby systemy sztucznej inteligencji obciążone wysokim ryzykiem podlegały takim samym wymogom w zakresie przejrzystości i informacji dla osób fizycznych, jak ma to obecnie miejsce w przypadku użytkowników.
12. Zwraca uwagę na główne zagrożenia i konsekwencje dla praw człowieka związane ze stosowaniem klasyfikacji społecznych.
13. W tym kontekście bardzo sceptycznie podchodzi do dwóch wymienionych w rozporządzeniu<sup>(2)</sup> przesłanek, na podstawie których ustala się, kiedy klasyfikacja społeczna prowadzi do krzywdzącego lub niekorzystnego traktowania osób lub grup osób, ponieważ ustalenie istnienia takich powodów jest niezwykle trudne. W związku z tym Komitet wzywa do jasnego sformułowania silnych zabezpieczeń, aby zapobiec obchodzeniu zakazu stosowania praktyk klasyfikacji społecznej.

(1) [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_en)

(2) Artykuł 5 ustęp 1 litera c).

14. Zauważa, że motywacje rozporządzenia odnoszą się do zagrożeń, na jakie narażone są osoby fizyczne w wyniku ich interakcji z systemami AI wysokiego ryzyka w kontekście m.in. kształcenia, szkolenia, zatrudnienia, zarządzania zasobami ludzkimi, dostępu do samozatrudnienia lub dostępu do niektórych podstawowych usług prywatnych i publicznych oraz korzystania z nich.

15. Wzywa Komisję do dalszego badania kwalifikacji systemów AI wysokiego ryzyka przeznaczonych do użytku przez organy publiczne<sup>(3)</sup>.

16. Apeluje, by jakiś organ udzielał ważnych porad ex ante dotyczących interpretacji przepisów rozporządzenia, również w odniesieniu do ogólnego rozporządzenia o ochronie danych. Zwiększa to pewność prawa i zmniejsza koszty projektowania i wdrażania systemów AI.

17. Podkreśla w związku z tym znaczenie jasności w sformułowaniu rozporządzenia, które ma zasadnicze znaczenie dla budowy ekosystemu zaufania i zniesienia niepewności prawa związanej z rozwojem i stosowaniem systemów AI. Pozwoliłoby to uniknąć błędnej interpretacji proponowanych wymogów i zminimalizować ryzyko późniejszego niewłaściwego zarządzania aplikacjami AI, a tym samym zmaksymalizować skuteczność i wiarygodność sankcji przewidzianych w rozporządzeniu. Jednocześnie, zgodnie z programem Komisji Europejskiej na rzecz lepszego stanowienia prawa, kluczowe znaczenie ma wczesne wykrywanie i eliminowanie potencjalnych przypadków pokrywania się obowiązujących przepisów i konfliktów między nimi.

18. Zauważa, że wiele władz lokalnych i regionalnych wykorzystuje te same systemy AI do podobnych zadań. W zdecydowanej większości przypadków systemy te są projektowane przez firmy prywatne.

19. Zwraca uwagę, że wniosek dotyczący rozporządzenia nie jest jedyny, jeśli chodzi o zagwarantowanie praw obywatelskich, lecz musi być rozpatrywany w powiązaniu z istniejącym prawodawstwem. Zachęca się zatem państwa członkowskie do zapewniania na bieżąco niezbędnych środków administracyjnych, aby zajmować się szansami i zagrożeniami związanymi ze stosowaniem AI w sektorze publicznym.

20. Zauważa, że oznacza to, iż w ramach oceny zgodności przepisy europejskie i krajowe są interpretowane przez przedsiębiorstwa i jednostki notyfikowane, a tym samym mają wpływ na praktykę władz lokalnych i regionalnych, które korzystają z tych systemów AI. Utrudnia to określenie, w jakim stopniu polityka lokalna i regionalna może zostać dodana do tych systemów AI. W związku z tym Komitet zwraca uwagę na szczególne potrzeby władz lokalnych i regionalnych oraz na to, że uniwersalne podejście może osłabić skuteczność systemów AI w reagowaniu na te potrzeby. Ponadto proponuje, aby rozporządzenie upoważniało państwa członkowskie do regulowania systemów sztucznej inteligencji wysokiego ryzyka na podstawie nadrzędnych i uzasadnionych względów interesu publicznego.

21. Apeluje w związku z tym o przejrzystość i dostępność ocen zgodności dla ogółu społeczeństwa. Ponadto władze lokalne i regionalne powinny również mieć możliwość uczestniczenia w monitorowaniu systemów AI, składania sprawozdań z ich wdrażania w terenie oraz formalnego wkładu w ocenę stosowania rozporządzenia przez Komisję Europejską.

22. Podkreśla, że stosowanie piaskownicy regulacyjnej wymaga ustanowienia odpowiednich prawnych, metodologicznych i etycznych warunków umożliwiających rozwój technologii, prawodawstwa i oceny prawodawstwa oraz że należy ustanowić jasne kryteria dopuszczania przedsiębiorców do piaskownicy regulacyjnej. Aby zapewnić organizacjom konsumenckim możliwość egzekwowania przepisów aktu w sprawie sztucznej inteligencji, należy go dodać do załącznika I do europejskiej dyrektywy w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów ((UE) 2020/1828).

### **Kampanie informacyjne**

23. Podkreśla znaczenie kampanii publicznych, tak aby ogół społeczeństwa był informowany o istnieniu i użyteczności systemów sztucznej inteligencji oraz o potencjalnych zagrożeniach, a także zaznajamiany z nimi. Podkreśla, że istnieje pilna potrzeba przekazywania konsumentom wyczerpujących informacji na temat procesów decyzyjnych sterowanych przez sztuczną inteligencję / maszyny. W związku z tym zwraca się do Komisji Europejskiej o zapewnienie finansowania takich kampanii.

<sup>(3)</sup> Załącznik III pkt 5 lit. a).

**Obciążenia administracyjne**

24. Wyraża zaniepokojenie potencjalnymi obciążeniami administracyjnymi wynikającymi z proponowanego rozporządzenia. Obciążenia administracyjne mogą utrudniać małym i średnim przedsiębiorstwom oraz władzom lokalnym i regionalnym promowanie innowacji i wdrażanie systemów AI <sup>(4)</sup>.

**Zasady proporcjonalności i pomocniczości**

25. Uważa, że projekt rozporządzenia jest zgodny z wymogami zasad proporcjonalności i pomocniczości. Wartość dodana działań UE w tej dziedzinie oraz stosowność podstaw prawnych wybranych przez Komisję są jasne i spójne. Ocena skutków zawierała odrębną sekcję dotyczącą pomocniczości. Ponadto żaden parlament narodowy nie wydał uzasadnionej opinii w sprawie nieprzestrzegania zasady pomocniczości w terminie składania wniosków wyznaczonym na dzień 2 września 2021 r.

Bruksela, dnia 2 grudnia 2021 r.

Apostolos TZITZIKOSTAS

*Przewodniczący  
Europejskiego Komitetu Regionów*

---

<sup>(4)</sup> W niedawnym badaniu zleconym przez Komisję Europejską (*Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, s. 12) oszacowano, że przy rozsądnych założeniach uzyskanie certyfikatu dla systemu AI może kosztować średnio 16 800–23 000 EUR, co stanowi ok. 10–14 % kosztów opracowania systemu.