EROD–EIOD

Wspólna opinia 5/2021

w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji („akt w sprawie sztucznej inteligencji”)

18 czerwca 2021 r.

Streszczenie

W dniu 21 kwietnia 2021 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (zwany dalej „wnioskiem"). EROD i EIOD z zadowoleniem przyjmują troskę prawodawcy o wykorzystanie sztucznej inteligencji w Unii Europejskiej (UE) i podkreślają, że wniosek ma szczególnie istotny **wpływ na ochronę danych**.

EROD i EIOD zauważają, że **podstawą prawną** wniosku jest przede wszystkim art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Ponadto wniosek opiera się również na art. 16 TFUE w zakresie, w jakim zawiera on przepisy szczegółowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, w szczególności ograniczenia wykorzystywania systemów sztucznej inteligencji do zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa. EROD i EIOD przypominają, że zgodnie z orzecznictwem Trybunału Sprawiedliwości UE (TSUE) art. 16 TFUE stanowi odpowiednią podstawę prawną w przypadkach, w których ochrona danych osobowych jest jednym z zasadniczych celów lub elementów przepisów przyjętych przez unijnego prawodawcę. Stosowanie art. 16 TFUE wiąże się również z **koniecznością zapewnienia niezależnego nadzoru nad przestrzeganiem** wymogów dotyczących przetwarzania danych osobowych, co jest również wymagane na mocy art. 8 Karty praw podstawowych UE.

Jeśli chodzi o **zakres wniosku**, EROD i EIOD z dużym zadowoleniem przyjmują fakt, że obejmuje on dostarczanie i wykorzystywanie systemów sztucznej inteligencji przez instytucje, organy lub jednostki organizacyjne UE. **Wyłączenie międzynarodowej współpracy organów ścigania z zakresu** wniosku budzi jednak poważne obawy EROD i EIOD, ponieważ takie wyłączenie stwarza znaczne ryzyko obchodzenia przepisów (np. państwa trzecie lub organizacje międzynarodowe obsługujące aplikacje wysokiego ryzyka, na których polegają organy publiczne w UE).

EROD i EIOD **z zadowoleniem przyjmują podejście oparte na analizie ryzyka**, które stanowi podstawę wniosku. Należy jednak doprecyzować to podejście i dostosować pojęcie „zagrożenia dla praw podstawowych" do przepisów RODO i rozporządzenia (UE) 2018/1725 (EUDPR), ponieważ w grę wchodzą aspekty związane z ochroną danych osobowych.

Ponadto EROD i EIOD zgadzają się z wnioskiem, który stanowi, że sklasyfikowanie **systemu sztucznej inteligencji jako systemu wysokiego ryzyka niekoniecznie oznacza, że jest on sam w sobie zgodny z prawem** i jako taki może zostać wdrożony przez użytkownika. **Może zaistnieć konieczność spełnienia** przez administratora danych **dalszych wymogów wynikających z unijnych przepisów o ochronie danych**. Ponadto przestrzeganie zobowiązań prawnych wynikających z przepisów Unii (w tym w zakresie ochrony danych osobowych) powinno być warunkiem wstępnym dopuszczenia do obrotu na rynku europejskim produktu z oznakowaniem zgodności CE. W związku z tym EROD i EIOD uważają, że **wymóg zapewnienia zgodności z przepisami RODO i EUDPR powinien zostać uwzględniony w rozdziale 2 tytułu III**. Ponadto EROD i EIOD uważają, że konieczne jest dostosowanie procedury oceny zgodności zawartej we wniosku w taki sposób, aby osoby trzecie zawsze przeprowadzały oceny zgodności *ex ante* systemów sztucznej inteligencji wysokiego ryzyka.

Ze względu na duże ryzyko dyskryminacji we wniosku zakazuje się „punktowej oceny zachowań społecznych", gdy jest ona prowadzona „przez określony czas" lub „przez organy publiczne lub w ich imieniu". Jednak prywatne przedsiębiorstwa, takie jak dostawcy mediów społecznościowych i usług w chmurze, również mogą przetwarzać ogromne ilości danych osobowych i prowadzić punktową ocenę

zachowań społecznych. W związku z tym **w przyszłym rozporządzeniu w sprawie sztucznej inteligencji należy zakazać prowadzenia wszelkiego rodzaju punktowej oceny zachowań społecznych**.

Zdalna identyfikacja biometryczna osób w przestrzeni publicznej wiąże się z wysokim ryzykiem ingerencji w życie prywatne osób fizycznych, co może mieć poważny wpływ na oczekiwanie obywateli co do zachowania anonimowości w przestrzeni publicznej. Z tych powodów EROD i EIOD **wzywają do wprowadzenia ogólnego zakazu jakiegokolwiek wykorzystywania sztucznej inteligencji do automatycznego rozpoznawania cech ludzkich w przestrzeni publicznej** – takich jak twarze, lecz również chód, odciski palców, DNA, głos, uderzenia w klawisze i inne sygnały biometryczne lub behawioralne – w jakimkolwiek kontekście. Zaleca się również wprowadzenie **zakazu** stosowania **systemów sztucznej inteligencji, które kategoryzują osoby fizyczne w klastry na podstawie danych biometrycznych** według pochodzenia etnicznego, płci, a także orientacji politycznej lub seksualnej lub innych przyczyn dyskryminacji przewidzianych w art. 21 Karty. Ponadto EROD i EIOD uważają, że wykorzystanie sztucznej inteligencji do **wyciągania wniosków na temat stanu emocjonalnego danej osoby fizycznej jest wysoce niepożądane i powinno być zakazane**.

EROD i EIOD z zadowoleniem przyjmują **wyznaczenie EIOD jako organu właściwego i organu nadzoru rynku do celów nadzoru nad instytucjami, organami i jednostkami organizacyjnymi Unii**. Należy jednak doprecyzować rolę i zadania EIOD, zwłaszcza jeśli chodzi o jego rolę jako organu nadzoru rynku. Ponadto w przyszłym rozporządzeniu w sprawie sztucznej inteligencji należy wyraźnie ustalić **niezależność organów nadzorczych** w wykonywaniu ich zadań związanych z nadzorem i egzekwowaniem przepisów.

Wyznaczenie organów ochrony danych jako krajowych organów nadzorczych zapewniłoby bardziej zharmonizowane podejście regulacyjne i przyczyniłoby się do spójnej interpretacji przepisów dotyczących przetwarzania danych oraz uniknięcia sprzeczności w zakresie ich egzekwowania przez państwa członkowskie. W związku z tym EROD i EIOD uważają, że **organy ochrony danych powinny zostać wyznaczone jako krajowe organy nadzorcze zgodnie z art. 59 wniosku**.

We wniosku powierza się Komisji dominującą rolę w „Europejskiej Radzie ds. Sztucznej Inteligencji" (EAIB). Rola ta jest sprzeczna z koniecznością zapewnienia niezależności europejskiego organu ds. sztucznej inteligencji od jakichkolwiek wpływów politycznych. Aby zapewnić jego niezależność, w ramach przyszłego rozporządzenia w sprawie sztucznej inteligencji należy nadać **EAIB większą autonomię** i zagwarantować jej możliwość działania z własnej inicjatywy.

Biorąc pod uwagę rozpowszechnienie systemów sztucznej inteligencji na całym jednolitym rynku oraz prawdopodobieństwo wystąpienia przypadków transgranicznych, istnieje zasadnicza potrzeba zharmonizowanego egzekwowania przepisów oraz właściwego podziału kompetencji pomiędzy krajowymi organami nadzorczymi. EROD i EIOD sugerują, że należy rozważyć wprowadzenie **mechanizmu gwarantującego pojedynczy punkt kontaktowy dla osób fizycznych objętych tymi przepisami oraz przedsiębiorstw w odniesieniu do każdego systemu sztucznej inteligencji.**

Jeśli chodzi o **piaskownice**, EROD i EIOD **zalecają doprecyzowanie ich zakresu i celów**. We wniosku należy również wyraźnie wskazać, że podstawa prawna takich piaskownic powinna być zgodna z wymogami ustanowionymi w istniejących ramach ochrony danych.

System certyfikacji przedstawiony we wniosku **nie ma wyraźnego związku z unijnymi przepisami o ochronie danych**, jak również z innymi przepisami Unii i państw członkowskich mającymi zastosowanie do każdego „obszaru" systemu sztucznej inteligencji wysokiego ryzyka i nie uwzględnia **zasad**

minimalizacji danych i ochrony danych w fazie projektowania jako jednego z aspektów, które należy wziąć pod uwagę **przed uzyskaniem oznakowania zgodności CE**. W związku z tym EROD i EIOD zalecają zmianę wniosku w celu wyjaśnienia związku między certyfikatami wydawanymi na mocy wspomnianego rozporządzenia a certyfikatami, znakami jakości i oznaczeniami w zakresie ochrony danych. Ponadto organy ochrony danych powinny być zaangażowane w przygotowanie i ustanowienie zharmonizowanych norm i wspólnych specyfikacji.

W odniesieniu do **kodeksów postępowania** EROD i EIOD uważają za **konieczne wyjaśnienie**, czy ochrona danych osobowych ma być uważana za jeden z „wymogów dodatkowych", które mogą być uwzględnione w tych kodeksach postępowania, oraz zapewnienie, by „specyfikacje i rozwiązania techniczne" nie były sprzeczne z zasadami i regułami istniejących unijnych ram ochrony danych.

SPIS TREŚCI

Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych

uwzględniając art. 42 ust. 2 rozporządzenia (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE[1],

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[2],

uwzględniając wniosek o wydanie wspólnej opinii Europejskiego Inspektora Ochrony Danych i Europejskiej Rady Ochrony Danych z dnia 22 kwietnia 2021 r. w sprawie wniosku dotyczącego rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji),

PRZYJMUJĄ NINIEJSZĄ WSPÓLNĄ OPINIĘ

1 WPROWADZENIE

1. Pojawienie się systemów sztucznej inteligencji („SI") jest bardzo ważnym etapem rozwoju technologii i sposobu, w jaki ludzie z nich korzystają. Sztuczna inteligencja to zestaw kluczowych technologii, które w znacznym stopniu zmienią nasze codzienne życie, zarówno z punktu widzenia społecznego, jak i ekonomicznego. Oczekuje się, że w ciągu najbliższych kilku lat podjęte zostaną stanowcze decyzje w sprawie sztucznej inteligencji, ponieważ pomaga nam ona przezwyciężyć niektóre z największych wyzwań, z jakimi obecnie mierzymy się w wielu dziedzinach, począwszy od zdrowia po mobilność, czy od administracji publicznej po edukację.

2. Te obiecane zmiany nie są jednak pozbawione ryzyka. Ryzyko to jest rzeczywiście istotne, biorąc pod uwagę fakt, że skutki działania systemów sztucznej inteligencji zarówno dla ludzi, jak i społeczeństw są jeszcze w dużej mierze nieznane. Tworzenie treści, przewidywanie lub podejmowanie decyzji w sposób zautomatyzowany, jak to czynią systemy sztucznej inteligencji, za pomocą technik uczenia maszynowego lub reguł wnioskowania logicznego i probabilistycznego, nie jest tożsame z wykonywaniem tych czynności przez człowieka, za pomocą rozumowania twórczego lub teoretycznego, ponoszącego pełną odpowiedzialność za ich skutki.

3. Sztuczna inteligencja przyczyni się do zwiększenia liczby przewidywań, które można wykonać w wielu dziedzinach, poczynając od mierzalnych korelacji między danymi, niewidocznych dla ludzkich oczu, ale widocznych dla maszyn, które ułatwiają nam życie i pomagają rozwiązać wiele problemów, lecz jednocześnie osłabią naszą zdolność do interpretacji związku

[1] Dz.U. L 295 z 21.11.2018, s. 39–98.
[2] Odniesienia do „państw członkowskich" w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".

przyczynowego wyników, w taki sposób, że pojęcia przejrzystości, ludzkiej kontroli, rozliczalności i odpowiedzialności za wyniki zostaną poważnie zakwestionowane.

4. Dane (osobowe i nieosobowe) w systemach sztucznej inteligencji stanowią w wielu przypadkach kluczową przesłankę autonomicznego podejmowania decyzji, które nieuchronnie wpłyną na życie osób fizycznych w różnych sferach. W związku z tym EROD i EIOD już na tym etapie zdecydowanie twierdzą, że wniosek dotyczący rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji („akt w sprawie sztucznej inteligencji") (zwany dalej „wnioskiem")[3] ma **istotne znaczenie dla kwestii ochrony danych**.

5. Powierzenie maszynom zadania podejmowania decyzji na podstawie danych stworzy zagrożenia dla praw i wolności osób fizycznych, wpłynie na ich życie prywatne i może zaszkodzić grupom społecznym, a nawet całemu społeczeństwu. EROD i EIOD podkreślają, że prawa do życia prywatnego i ochrony danych osobowych, sprzeczne z założeniem autonomicznego podejmowania decyzji przez maszyny leżącym u podstaw koncepcji sztucznej inteligencji, są filarem wartości UE uznanych w Powszechnej deklaracji praw człowieka (art. 12), Europejskiej konwencji praw człowieka (art. 8) i Karcie praw podstawowych UE (zwanej dalej „Kartą") (art. 7 i 8). Pogodzenie perspektywy rozwoju oferowanej przez aplikacje oparte na sztucznej inteligencji z centralnym znaczeniem i prymatem człowieka wobec maszyn jest bardzo ambitnym, lecz koniecznym celem.

6. EROD i EIOD z zadowoleniem przyjmują zaangażowanie w regulację wszystkich zainteresowanych stron łańcucha wartości sztucznej inteligencji oraz wprowadzenie szczegółowych wymogów dla dostawców rozwiązań, ponieważ odgrywają oni znaczącą rolę w dostarczaniu produktów wykorzystujących ich systemy. Należy jednak jasno określić i przypisać obowiązki poszczególnym stronom – użytkownikowi, dostawcy, importerowi lub dystrybutorowi systemu sztucznej inteligencji. W szczególności, podczas przetwarzania danych osobowych, należy zwrócić szczególną uwagę na spójność tych ról i obowiązków z pojęciami administratora danych i podmiotu przetwarzającego dane, zawartymi w ramach ochrony danych, ponieważ obie normy nie są ze sobą zgodne.

7. We wniosku ważne miejsce zajmuje pojęcie „nadzoru ze strony człowieka" (art. 14), które EROD i EIOD przyjmują z zadowoleniem. Jednakże, jak stwierdzono wcześniej, ze względu na znaczący potencjalny wpływ niektórych systemów sztucznej inteligencji na osoby fizyczne lub grupy osób, rzeczywista centralna rola człowieka powinna opierać się na wysoce specjalistycznym nadzorze ze strony człowieka i zgodnym z prawem przetwarzaniu danych w zakresie, w jakim systemy te opierają się na przetwarzaniu danych osobowych lub przetwarzają dane osobowe w celu realizacji swoich zadań, tak aby zapewnić przestrzeganie prawa do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu danych.

8. Ponadto, ze względu na szczególnie wrażliwy charakter wielu aplikacji opartych na sztucznej inteligencji, w ramach wniosku należy zachęcać do przyjęcia podejścia uwzględniającego ochronę danych w fazie projektowania i domyślną ochronę danych na każdym poziomie,

[3] COM(2021)206 final.

zachęcając do skutecznego wprowadzania przepisów o ochronie danych (przewidzianych w art. 25 RODO i art. 27 EUDPR) za pomocą najnowocześniejszych technologii.

9. Ponadto EROD i EIOD podkreślają, że niniejsza wspólna opinia została przedstawiona jedynie jako wstępna analiza wniosku, bez uszczerbku dla jakiejkolwiek dalszej oceny i opinii na temat skutków wniosku i jego zgodności z unijnymi przepisami o ochronie danych.

2 ANALIZA KLUCZOWYCH ZASAD PRZEDSTAWIONYCH WE WNIOSKU

2.1 Zakres wniosku i związek z istniejącymi ramami prawnymi

10. Zgodnie z uzasadnieniem **podstawą prawną** wniosku jest przede wszystkim art. 114 TFUE, w którym przewidziano przyjęcie środków mających na celu zapewnienie ustanowienia i funkcjonowania rynku wewnętrznego[4]. Ponadto wniosek opiera się na art. 16 TFUE *w zakresie, w jakim zawiera on przepisy szczegółowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych*, w szczególności ograniczenia wykorzystywania systemów sztucznej inteligencji do zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa[5].

11. EROD i EIOD przypominają, że zgodnie z orzecznictwem TSUE art. 16 TFUE stanowi odpowiednią podstawę prawną w przypadkach, w których ochrona danych osobowych jest jednym z zasadniczych celów lub elementów przepisów przyjętych przez prawodawcę UE[6]. Stosowanie art. 16 TFUE wiąże się również z koniecznością zapewnienia niezależnego nadzoru nad przestrzeganiem wymogów dotyczących przetwarzania danych osobowych, co jest również wymagane na mocy art. 8 Karty.

12. EIOD i EROD przypominają, że istnieją już kompleksowe ramy ochrony danych przyjęte na podstawie art. 16 TFUE, na które składają się ogólne rozporządzenie o ochronie danych (RODO)[7], rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne UE (EUDPR)[8] oraz dyrektywa (UE) 2016/680 (LED)[9]. Zgodnie z wnioskiem jedynie dodatkowe ograniczenia

[4] Uzasadnienie, s. 5.
[5] Uzasadnienie, s. 6. Zob. również motyw 2 wniosku.
[6] Opinia z dnia 26 lipca 2017 r., *PNR Kanada*, procedura opiniowania 1/15, ECLI:EU:C:2017:592, pkt 96.
[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1–88).
[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE, Dz.U. L 295 z 21.11.2018, s. 39–98.
[9] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89–131).

dotyczące przetwarzania danych biometrycznych zawarte we wniosku można uznać za oparte na art. 16 TFUE, a zatem za mające tę samą podstawę prawną co RODO, EUDPR lub LED. Ma to istotny wpływ na związek wniosku z przepisami RODO, EUDPR i ogólnie LED, jak przedstawiono poniżej.

13. Jeśli chodzi o **zakres wniosku** EROD i EIOD z dużym zadowoleniem przyjmują fakt, że zakres wniosku rozszerzono również do wykorzystywania systemów sztucznej inteligencji przez instytucje, organy lub jednostki organizacyjne UE. Biorąc pod uwagę, że wykorzystywanie systemów sztucznej inteligencji przez te podmioty może mieć również istotny wpływ na prawa podstawowe osób fizycznych, podobnie jak ma to miejsce w państwach członkowskich, niezbędne jest, aby nowe ramy regulacyjne dotyczące sztucznej inteligencji miały zastosowanie zarówno do państw członkowskich, jak i do instytucji, organów i jednostek organizacyjnych UE, w celu zapewnienia spójnego podejścia w całej Unii. Ponieważ instytucje, organy i jednostki organizacyjne UE mogą działać zarówno jako dostawcy, jak i użytkownicy systemów sztucznej inteligencji, EIOD i EROD uważają za w pełni stosowne objęcie tych podmiotów zakresem wniosku na podstawie art. 114 TFUE.

14. EROD i EIOD mają jednak poważne obawy co do wyłączenia międzynarodowej współpracy w zakresie egzekwowania prawa z zakresu zastosowania przewidzianego w art. 2 ust. 4 wniosku. Wyłączenie to stwarza znaczne ryzyko obchodzenia przepisów (np. państwa trzecie lub organizacje międzynarodowe obsługujące aplikacje wysokiego ryzyka, na których polegają organy publiczne w UE).

15. Rozwój i wykorzystanie systemów sztucznej inteligencji w wielu przypadkach będą wiązały się z przetwarzaniem danych osobowych. Niezwykle ważne jest zapewnienie jasności co do związku niniejszego wniosku z obowiązującymi przepisami Unii w zakresie ochrony danych. Wniosek pozostaje bez uszczerbku dla przepisów RODO, EUDPR i LED oraz stanowi ich uzupełnienie. Chociaż w motywach wniosku wyjaśniono, że wykorzystanie systemów sztucznej inteligencji powinno nadal być zgodne z przepisami o ochronie danych, **EROD i EIOD zdecydowanie zalecają wyjaśnienie w art. 1 wniosku, że przepisy Unii dotyczące ochrony danych osobowych**, w szczególności RODO, EUDPR, dyrektywa o prywatności i łączności elektronicznej[10] oraz LED, mają zastosowanie do każdego przetwarzania danych osobowych objętego zakresem wniosku. W odnośnym motywie również należy doprecyzować, że wniosek nie będzie miał wpływu na stosowanie obowiązujących przepisów Unii regulujących przetwarzanie danych osobowych, w tym na zadania i uprawnienia niezależnych organów nadzorczych właściwych do monitorowania zgodności z tymi aktami.

[10] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), zmieniona dyrektywą 2006/24/WE i dyrektywą 2009/136/WE.

2.2 Podejście oparte na analizie ryzyka

16. EROD i EIOD **z zadowoleniem przyjmują podejście oparte na analizie ryzyka**, które stanowi podstawę wniosku. Wniosek miałby zastosowanie do wszystkich systemów sztucznej inteligencji, w tym tych, które nie wiążą się z przetwarzaniem danych osobowych, ale mogą mieć wpływ na interesy lub podstawowe prawa i wolności.

17. EROD i EIOD zauważają, że niektóre przepisy wniosku pomijają zagrożenia dla grup osób fizycznych lub społeczeństwa jako całości (np. skutki zbiorowe o szczególnym znaczeniu, takie jak dyskryminacja grupowa lub wyrażanie opinii politycznych w przestrzeni publicznej). EROD i EIOD zalecają, aby odpowiednio ocenić i złagodzić zagrożenia społeczne/zagrożenia dla grup osób, jakie stwarzają systemy sztucznej inteligencji.

18. EROD i EIOD są zdania, że należy doprecyzować oparte na analizie ryzyka podejście przedstawione we wniosku, a pojęcie „zagrożenia dla praw podstawowych" należy **dostosować do przepisów RODO**, o ile w grę wchodzą aspekty związane z ochroną danych osobowych. Niezależnie od tego, czy są to użytkownicy końcowi, osoby, których dane dotyczą, czy inne osoby, których dotyczy system sztucznej inteligencji, brak w tekście jakiegokolwiek odniesienia do osoby, na którą system sztucznej inteligencji ma wpływ, wydaje się niedopatrzeniem we wniosku. W istocie zobowiązania nałożone na podmioty wobec tych osób powinny wynikać w sposób bardziej konkretny z ochrony osób fizycznych i ich praw. W związku z tym EROD i EIOD wzywają prawodawców do wyraźnego uwzględnienia we wniosku **praw i środków prawnych przysługujących osobom** podlegających systemom sztucznej inteligencji.

19. EROD i EIOD przyjmują do wiadomości wybór polegający na przedstawieniu wyczerpującego wykazu **systemów sztucznej inteligencji wysokiego ryzyka**. Wybór ten może spowodować czarno-biały efekt, ze słabą zdolnością przyciągania w sytuacjach wysokiego ryzyka, podważając ogólne podejście oparte na analizie ryzyka leżące u podstaw wniosku. Ponadto w wykazie systemów sztucznej inteligencji wysokiego ryzyka wyszczególnionym w załącznikach II i III do wniosku brakuje niektórych rodzajów przypadków użycia, które wiążą się ze znacznym ryzykiem, takich jak wykorzystanie sztucznej inteligencji do określania składki ubezpieczeniowej lub do oceny leczenia bądź do celów badań w dziedzinie zdrowia. EROD i EIOD podkreślają również, że załączniki te będą musiały być regularnie aktualizowane w celu zagwarantowania, że ich zakres jest odpowiedni.

20. Zgodnie z wnioskiem **dostawcy** systemu sztucznej inteligencji muszą przeprowadzić ocenę ryzyka, jednak w większości przypadków administratorami (danych) będą raczej **użytkownicy** niż dostawcy systemów sztucznej inteligencji (np. użytkownik systemu rozpoznawania twarzy jest „administratorem" i dlatego nie jest związany wymogami dotyczącymi dostawców systemów sztucznej inteligencji wysokiego ryzyka przewidzianymi we wniosku).

21. Ponadto **dostawca nie zawsze będzie miał możliwość oceny wszystkich zastosowań** systemu sztucznej inteligencji. W związku z tym wstępna ocena ryzyka będzie miała bardziej ogólny charakter niż ocena dokonywana przez użytkownika systemu sztucznej inteligencji. Nawet jeżeli wstępna ocena ryzyka przeprowadzona przez dostawcę nie wskazuje, że system

sztucznej inteligencji jest systemem „wysokiego ryzyka" zgodnie z wnioskiem, nie powinno to wykluczać **późniejszej (bardziej szczegółowej) oceny** (oceny skutków dla ochrony danych na mocy art. 35 RODO, art. 39 EUDPR lub art. 27 LED) **, którą powinien przeprowadzić użytkownik systemu**, biorąc pod uwagę kontekst użycia i konkretne przypadki użycia. Interpretacja tego, czy zgodnie z przepisami RODO, EUDPR i LED dany rodzaj przetwarzania może powodować wysokie ryzyko powinna być dokonywana niezależnie od wniosku. Jednakże sklasyfikowanie systemu sztucznej inteligencji jako stwarzającego „wysokie ryzyko" ze względu na jego wpływ na prawa podstawowe[11] **wywołuje domniemanie „wysokiego ryzyka" na mocy przepisów RODO, EUDPR i LED w zakresie, w jakim przetwarzane są dane osobowe.**

22. **EROD i EIOD zgadzają się z wnioskiem, który stanowi, że sklasyfikowanie systemu sztucznej inteligencji jako systemu wysokiego ryzyka niekoniecznie oznacza, że jest on sam w sobie zgodny z prawem i jako taki może zostać wdrożony przez użytkownika. Może zaistnieć konieczność spełnienia przez administratora danych dalszych wymogów wynikających z unijnych przepisów o ochronie danych.** Ponadto argumentacja leżąca u podstaw art. 5 wniosku, zgodnie z którą, w przeciwieństwie do systemów zakazanych, systemy wysokiego ryzyka mogą być zasadniczo dopuszczalne, powinna zostać omówiona i wyjaśniona we wniosku, zwłaszcza że proponowane oznakowanie zgodności CE nie oznacza, że związane z nim przetwarzanie danych osobowych jest zgodne z prawem.

23. Spełnienie zobowiązań prawnych wynikających z przepisów Unii (w tym dotyczących ochrony danych osobowych) powinno być jednak warunkiem wstępnym dopuszczenia do obrotu na rynku europejskim produktu z oznaczeniem zgodności CE. W związku z tym EROD i EIOD **zalecają włączenie do rozdziału 2 tytułu III wniosku wymogu zapewnienia zgodności z przepisami RODO i EUDPR**. Wymogi te podlegają audytowi (audytowi przeprowadzanemu przez osobę trzecią) przed nadaniem oznakowania zgodności CE zgodnie z zasadą rozliczalności. W kontekście tej oceny dokonanej przez osobę trzecią szczególnie istotna będzie wstępna ocena skutków, którą ma przeprowadzić dostawca.

24. Mając na uwadze złożoność wynikającą z rozwoju systemów sztucznej inteligencji, należy wskazać, że charakterystyka techniczna systemów sztucznej inteligencji (np. rodzaj podejścia w zakresie sztucznej inteligencji) może powodować większe ryzyko. Dlatego też każda ocena ryzyka systemu sztucznej inteligencji powinna uwzględniać **charakterystykę techniczną** wraz **z konkretnymi przypadkami użycia oraz kontekstem**, w którym ten system działa.

25. W świetle powyższego EROD i EIOD zalecają wskazanie we wniosku, że **dostawca** powinien przeprowadzić wstępną ocenę ryzyka w odniesieniu do danego systemu sztucznej inteligencji, **biorąc pod uwagę przypadki użycia** (które zostaną określone we wniosku – jako uzupełnienie

[11] Agencja Praw Podstawowych Unii Europejskiej (FRA) zajęła się już kwestią konieczności przeprowadzania ocen skutków dla praw podstawowych w przypadku wykorzystywania sztucznej inteligencji lub powiązanych technologii. W swoim sprawozdaniu z 2020 r. zatytułowanym „Naprawić przyszłość – Sztuczna inteligencja a prawa podstawowe" (*Getting the future right – Artificial intelligence and fundamental rights*) FRA wskazała „pułapki w stosowaniu sztucznej inteligencji, na przykład w prognozowaniu kryminologicznym, diagnozach lekarskich, usługach społecznych i reklamie ukierunkowanej" i podkreśliła, że „organizacje prywatne i publiczne powinny przeprowadzać oceny tego, w jaki sposób sztuczna inteligencja może zaszkodzić prawom podstawowym", aby ograniczyć jej negatywny wpływ na osoby fizyczne.

na przykład załącznika III pkt 1 lit. a), w którym przypadki użycia systemów biometrycznych opartych na sztucznej inteligencji nie zostały wymienione), oraz że **użytkownik** systemu sztucznej inteligencji, pełniący funkcję administratora danych na mocy unijnych przepisów o ochronie danych (w stosownych przypadkach), powinien przeprowadzić ocenę skutków dla ochrony danych zgodnie z art. 35 RODO, art. 39 EUDPR i art. 27 LED, uwzględniając nie tylko charakterystykę techniczną i **przypadek użycia**, lecz **również szczególny kontekst**, w którym system sztucznej inteligencji będzie działać.

26. Ponadto należy doprecyzować niektóre z pojęć wymienionych w załączniku III do wniosku, np. pojęcie „podstawowe usługi prywatne" lub pojęcie drobnych dostawców wykorzystujących sztuczną inteligencję do oceny zdolności kredytowej na własny użytek.

2.3 Zabronione zastosowania sztucznej inteligencji

27. EROD i EIOD uważają, że **inwazyjne formy sztucznej inteligencji** – zwłaszcza te, które mogą naruszać godność ludzką – powinny być postrzegane jako zakazane systemy sztucznej inteligencji zgodnie z art. 5 wniosku, a nie klasyfikowane jedynie jako systemy „wysokiego ryzyka" w załączniku III do wniosku, jak te objęte nr 6. Ma to zastosowanie w szczególności do porównań danych, które w dużej mierze dotyczą również osób, które nie dały żadnego powodu lub dały niewielki powód do obserwacji policyjnej, lub przetwarzania, które narusza zasadę ograniczenia celu zgodnie z przepisami o ochronie danych. Wykorzystanie sztucznej inteligencji w policji i organach ścigania wymaga ustanowienia specyficznych dla danego obszaru, precyzyjnych, przewidywalnych i proporcjonalnych zasad, które muszą uwzględniać interesy zainteresowanych osób oraz skutki dla funkcjonowania społeczeństwa demokratycznego.

28. Artykuł 5 wniosku stwarza ryzyko gołosłownych deklaracji na temat „wartości" i zakazu stosowania systemów sztucznej inteligencji sprzecznych z tymi wartościami. W rzeczywistości kryteria, o których mowa w art. 5, służące „kwalifikowaniu" systemów sztucznej inteligencji jako zakazanych, **ograniczają zakres zakazu** do tego stopnia, że w praktyce może się on okazać pozbawiony znaczenia (np. „powoduje lub może powodować [...] szkodę fizyczną lub psychiczną" w art. 5 ust. 1 lit. a) i b); ograniczenie do organów publicznych w art. 5 ust. 1 lit. c); niejasne sformułowanie w lit. c) ppkt (i) i (ii); ograniczenie wyłącznie do zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" bez jasnej definicji itd.).

29. W szczególności wykorzystanie sztucznej inteligencji do „punktowej oceny zachowań społecznych", przewidzianej w art. 5 ust. 1 lit. c) wniosku, może prowadzić do dyskryminacji i jest sprzeczne z podstawowymi wartościami UE. We wniosku zakazuje się tych praktyk tylko wtedy, gdy są one prowadzone „przez określony czas" lub „przez organy publiczne lub w ich imieniu". Prywatne przedsiębiorstwa, w szczególności dostawcy mediów społecznościowych i usług w chmurze, mogą przetwarzać ogromne ilości danych osobowych i prowadzić punktową ocenę zachowań społecznych. W związku z tym we **wniosku należy zakazać prowadzenia wszelkiego rodzaju punktowej oceny zachowań społecznych.** Należy zauważyć, że w kontekście egzekwowania prawa w art. 4 LED już w znacznym stopniu ograniczono – a w praktyce zakazano – tego rodzaju działań.

30. **Zdalna identyfikacja biometryczna** osób fizycznych w przestrzeni publicznej stwarza wysokie ryzyko ingerencji w życie prywatne tych osób. W związku z tym EROD i EIOD **uważają, że należy przyjąć bardziej rygorystyczne podejście**. Korzystanie z systemów sztucznej inteligencji może stwarzać poważne problemy związane z proporcjonalnością, ponieważ może wiązać się z przetwarzaniem danych ogromnej i nieproporcjonalnej liczby osób, których dane dotyczą, w celu identyfikacji jedynie kilku osób (np. pasażerów na lotniskach i stacjach kolejowych). **Nieskomplikowany** charakter systemów zdalnej identyfikacji biometrycznej stwarza również problemy związane z przejrzystością oraz problemy dotyczące podstawy prawnej przetwarzania danych na mocy prawa Unii (LED, RODO, EUDPR i inne obowiązujące przepisy). Nadal nierozwiązany pozostaje problem sposobu właściwego informowania osób fizycznych o tym przetwarzaniu, jak również skutecznego i terminowego wykonywania praw osób fizycznych. To samo dotyczy **nieodwracalnego, poważnego wpływu na** (uzasadnione) **oczekiwanie obywateli co do zachowania anonimowości w przestrzeni publicznej**, co ma bezpośredni negatywny wpływ na korzystanie z wolności wypowiedzi, zgromadzeń, zrzeszania się i przemieszczania się.

31. Artykuł 5 ust. 1 lit. d) wniosku zawiera obszerny **wykaz wyjątkowych przypadków**, w których zdalna identyfikacja biometryczna „w czasie rzeczywistym" w przestrzeni publicznej jest dozwolona do celów egzekwowania prawa. EROD i EIOD uważają **to podejście za wadliwe** pod kilkoma względami: Po pierwsze nie jest jasne, co należy rozumieć jako „znaczne opóźnienie" i w jaki sposób należy je uznać za okoliczność łagodzącą, biorąc pod uwagę fakt, że system identyfikacji masowej jest w stanie zidentyfikować tysiące osób w ciągu zaledwie kilku godzin. Ponadto inwazyjny charakter przetwarzania nie zawsze zależy od tego, czy identyfikacja odbywa się w czasie rzeczywistym, czy też nie. Zdalna identyfikacja biometryczna w kontekście protestu politycznego może wywołać efekt mrożący w odniesieniu do korzystania z podstawowych praw i wolności, takich jak wolność zgromadzeń i zrzeszania się, a także ogólnie z podstawowych zasad demokracji. Po drugie, inwazyjny charakter przetwarzania nie musi zależeć od jego celu. Wykorzystanie tego systemu do innych celów, takich jak ochrona prywatna, stanowi takie samo zagrożenie dla praw podstawowych w zakresie poszanowania życia prywatnego i rodzinnego oraz ochrony danych osobowych. Ponadto, nawet przy uwzględnieniu przewidzianych ograniczeń, potencjalna liczba podejrzanych lub sprawców przestępstw będzie prawie zawsze „wystarczająco wysoka", aby uzasadnić stałe wykorzystywanie systemów sztucznej inteligencji do wykrywania podejrzanych, pomimo dalszych warunków określonych w art. 5 ust. 2–4 wniosku. Zdaje się, że w uzasadnieniu wniosku pominięto fakt, że w przypadku monitorowania obszarów otwartych, obowiązki wynikające z unijnych przepisów o ochronie danych muszą być spełnione nie tylko w odniesieniu do podejrzanych, lecz w odniesieniu do wszystkich osób, które są w praktyce monitorowane.

32. Z tych wszystkich powodów EROD i EIOD **wzywają do wprowadzenia ogólnego zakazu jakiegokolwiek wykorzystywania sztucznej inteligencji do automatycznego rozpoznawania cech ludzkich w przestrzeni publicznej – takich jak twarze, lecz również chód, odciski palców, DNA, głos, uderzenia w klawisze i inne sygnały biometryczne lub behawioralne – w jakimkolwiek kontekście**. Obecne podejście przyjęte we wniosku polega na zidentyfikowaniu i sporządzeniu wykazu wszystkich systemów sztucznej inteligencji, które

powinny być zakazane. W związku z tym, aby zachować spójność, **systemy sztucznej inteligencji służące do zdalnej identyfikacji na dużą skalę w przestrzeni internetowej** powinny być zakazane zgodnie z art. 5 wniosku. Biorąc pod uwagę LED, EUDPR i RODO, EIOD i EROD nie są w stanie rozpoznać, w jaki sposób tego rodzaju praktyka mogłaby spełnić wymogi konieczności i proporcjonalności, które ostatecznie wynikają z tego, co TSUE i ETPC uznają za dopuszczalną ingerencję w prawa podstawowe.

33. Ponadto EROD i EIOD **zalecają wprowadzenie zakazu**, zarówno w odniesieniu do organów publicznych, jak i podmiotów prywatnych, dotyczącego stosowania **systemów sztucznej inteligencji kategoryzujących osoby fizyczne na podstawie danych biometrycznych (np. na podstawie rozpoznawania twarzy) w klastry według pochodzenia etnicznego, płci, a także orientacji politycznej lub seksualnej lub innych przyczyn dyskryminacji zakazanych na mocy art. 21 Karty, lub** systemów sztucznej inteligencji, których trafność nie została udowodniona lub które stoją w bezpośredniej sprzeczności z podstawowymi wartościami UE (np. poligraf, załącznik III, pkt 6. lit. b) i pkt 7. lit. a)). W związku z tym „**kategoryzacja biometryczna**" powinna być **zakazana na mocy art. 5**.

34. **Bycie określanym lub klasyfikowanym przez komputer odnośnie do przyszłego zachowania niezależnie od własnej woli narusza** również **godność ludzką.** Systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy ścigania w celu przeprowadzenia indywidualnej oceny ryzyka osób fizycznych na potrzeby oceny ryzyka popełnienia przez osobę fizyczną przestępstwa lub ponownego popełnienia przestępstwa, por. załącznik III, pkt 6. lit. a), lub w celu przewidywania wystąpienia lub ponownego wystąpienia rzeczywistego lub potencjalnego przestępstwa w oparciu o profilowanie osoby fizycznej lub ocenę cech osobowości i charakteru lub przeszłego zachowania przestępnego, por. załącznik III, pkt 6. lit. e), wykorzystywane zgodnie z ich przeznaczeniem doprowadzą do znacznego uprzedmiotowienia procesu podejmowania decyzji przez policję i organy sądowe, uprzedmiotawiając tym samym osobę, której takie decyzje dotyczą. Takie systemy sztucznej inteligencji naruszające istotę prawa do godności ludzkiej powinny być zakazane na mocy art. 5.

35. Ponadto EROD i EIOD uważają, że wykorzystanie sztucznej inteligencji do **wyciągania wniosków na temat stanu emocjonalnego danej osoby fizycznej jest wysoce niepożądane i powinno być zakazane,** z wyjątkiem pewnych ściśle określonych przypadków użycia, mianowicie do celów zdrowotnych lub badawczych (np. pacjenci, w przypadku których rozpoznawanie emocji ma istotne znaczenie), zawsze z zastosowaniem odpowiednich zabezpieczeń i oczywiście z zastrzeżeniem wszystkich innych warunków i ograniczeń w zakresie ochrony danych, w tym zasady ograniczenia celu.

2.4 Systemy sztucznej inteligencji wysokiego ryzyka

2.4.1 Potrzeba przeprowadzenia oceny zgodności *ex ante* przez osoby trzecie pochodzące z zewnątrz.

36. EROD i EIOD z zadowoleniem przyjmują fakt, że systemy sztucznej inteligencji, które stwarzają wysokie ryzyko, muszą być poddane uprzedniej ocenie zgodności, zanim zostaną wprowadzone do obrotu lub w inny sposób uruchomione w UE. Zasadniczo ten model regulacyjny przyjmuje się z zadowoleniem, ponieważ zapewnia on odpowiednią równowagę między czynnikami sprzyjającymi innowacji a wysokim poziomem proaktywnej ochrony praw podstawowych. Aby można je było wykorzystać w specyficznych środowiskach, takich jak procesy decyzyjne instytucji publicznych lub infrastruktury krytycznej, należy określić sposoby badania pełnego kodu źródłowego.

37. EROD i EIOD opowiadają się jednak za dostosowaniem procedury oceny zgodności zgodnie z art. 43 wniosku w taki sposób, aby **ocena zgodności *ex ante* osoby trzeciej była zasadniczo przeprowadzana w przypadku systemu sztucznej inteligencji wysokiego ryzyka**. Chociaż ocena zgodności osoby trzeciej przeprowadzana w przypadku przetwarzania danych osobowych wysokiego ryzyka nie jest wymogiem zawartym w RODO lub EUDPR, ryzyko stwarzane przez systemy sztucznej inteligencji nie zostało jeszcze w pełni poznane. Ogólne uwzględnienie obowiązku oceny zgodności osoby trzeciej zwiększyłoby zatem jeszcze bardziej pewność prawa i zaufanie do wszystkich systemów sztucznej inteligencji wysokiego ryzyka.

2.4.2 Zakres rozporządzenia musi również obejmować już wykorzystywane systemy sztucznej inteligencji

38. Zgodnie z art. 43 ust. 4 wniosku, systemy sztucznej inteligencji wysokiego ryzyka powinny podlegać nowej procedurze oceny zgodności w przypadku każdej znaczącej zmiany. Należy dopilnować, aby systemy sztucznej inteligencji spełniały wymogi przewidziane w rozporządzeniu w sprawie sztucznej inteligencji w całym cyklu ich życia. Systemy sztucznej inteligencji, które zostały wprowadzone do obrotu lub oddane do użytku przed rozpoczęciem stosowania proponowanego rozporządzenia (lub 12 miesięcy po tym terminie w przypadku wielkoskalowych systemów informatycznych wymienionych w załączniku IX), są wyłączone z jego zakresu, chyba że w systemach tych wprowadzono „znaczące zmiany” w zakresie projektu lub przeznaczenia (art. 83).

39. Próg „znaczących zmian” jest jednak niejasny. W motywie 66 wniosku określono niższy próg ponownej oceny zgodności „w przypadku każdej zmiany, która może mieć wpływ na zgodność”. Podobny próg byłby odpowiedni w przypadku art. 83, przynajmniej w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka. Ponadto, aby wyeliminować wszelkie luki w zakresie ochrony, konieczne jest, aby systemy sztucznej inteligencji, które zostały już utworzone i działają – po określonym etapie wdrożenia – również spełniały wszystkie wymogi rozporządzenia w sprawie sztucznej inteligencji.

40. Różnorodne możliwości przetwarzania danych osobowych i zagrożenia zewnętrzne wpływają również na bezpieczeństwo systemów sztucznej inteligencji. Zgodnie z art. 83 skupienie się na „znaczących zmianach w zakresie projektu lub przeznaczenia" systemu nie obejmuje odniesienia do zmian w zakresie zagrożeń zewnętrznych. W art. 83 wniosku należy zatem uwzględnić odniesienie do zmian scenariusza zagrożeń wynikających z zagrożeń zewnętrznych, np. cyberataków, wrogich ataków i uzasadnionych skarg konsumentów.

41. Ponadto, z uwagi na to, że przewidywana data rozpoczęcia stosowania wniosku to 24 miesiące po wejściu w życie przyszłego rozporządzenia, EIOD i EROD nie uważają za stosowne, aby systemy sztucznej inteligencji już wprowadzone do obrotu były wyłączone na jeszcze dłuższy okres czasu. Choć we wniosku przewiduje się również, że wymogi rozporządzenia są uwzględniane przy ocenie każdego wielkoskalowego systemu informatycznego zgodnie z aktami prawnymi wymienionymi w załączniku IX, EROD i EIOD uważają, że wymogi dotyczące oddania do użytku systemów sztucznej inteligencji powinny obowiązywać od daty rozpoczęcia stosowania przyszłego rozporządzenia.

2.5 Zarządzanie i Europejska Rada ds. Sztucznej Inteligencji

2.5.1 Zarządzanie

42. EROD i EIOD z zadowoleniem przyjmują fakt, że we wniosku wyznaczono EIOD jako organ właściwy i organ nadzoru rynku do celów nadzoru nad instytucjami, organami i jednostkami organizacyjnymi Unii, jeżeli są one objęte zakresem niniejszego wniosku. EIOD jest gotowy pełnić swoją nową rolę organu regulacyjnego ds. sztucznej inteligencji na potrzeby administracji publicznej UE. Ponadto rola i zadania EIOD nie zostały przedstawione w sposób wystarczająco szczegółowy i należy je dalej doprecyzować we wniosku, zwłaszcza jeśli chodzi o jego rolę jako organu nadzoru rynku.

43. EROD i EIOD uznają przydział środków finansowych, który w ramach wniosku przewidziano dla Rady i EIOD, występujących w charakterze organu notyfikującego. Wypełnianie nowych obowiązków przewidzianych dla EIOD, czy to w ramach pełnienia funkcji organu notyfikującego czy też nie, wymagałoby jednak znacznie większych zasobów finansowych i ludzkich.

44. Po pierwsze z uwagi na to, że w art. 63 ust. 6 stwierdza się, że EIOD „pełni rolę organu nadzoru rynku" w stosunku do instytucji, organów i jednostek organizacyjnych Unii objętych zakresem wniosku, co nie wyjaśnia, czy EIOD ma być uważany za pełnoprawny „organ nadzoru rynku", jak przewidziano w rozporządzeniu (UE) 2019/1020. Rodzi to pytania o obowiązki i uprawnienia EIOD w praktyce. Po drugie, o ile na pierwsze pytanie zostanie udzielona odpowiedź twierdząca, nie jest jasne, w jaki sposób rola EIOD przewidziana w EUDPR może sprostać zadaniom przewidzianym w art. 11 rozporządzenia (UE) 2019/1020, które obejmują „skuteczny nadzór rynku na swoim terytorium w odniesieniu do produktów udostępnianych online" lub „kontrole fizyczne i laboratoryjne oparte na odpowiednich próbkach". Istnieje ryzyko, że podjęcie się nowego zestawu zadań bez dalszych wyjaśnień zawartych we wniosku może zagrozić wypełnianiu obowiązków przez inspektora ochrony danych.

45. EROD i EIOD podkreślają jednak, że niektóre przepisy zawarte we wniosku określające zadania i uprawnienia różnych właściwych organów na mocy rozporządzenia w sprawie sztucznej inteligencji, ich relacje, charakter i gwarancję ich niezależności wydają się na tym etapie niejasne. Podczas gdy rozporządzenie 2019/1020 stanowi, że organ nadzoru rynku musi być niezależny, projekt rozporządzenia nie wymaga, by organy nadzorcze były niezależne, a nawet wymaga, by składały one Komisji sprawozdania z niektórych zadań wykonywanych przez organy nadzoru rynku, którymi mogą być różne instytucje. Ponieważ we wniosku stwierdza się również, że organy ochrony danych będą organami nadzoru rynku w odniesieniu do systemów sztucznej inteligencji wykorzystywanych do celów związanych z egzekwowaniem prawa (art. 63 ust. 5), oznacza to również, że będą one, być może za pośrednictwem krajowego organu nadzorczego, podlegać obowiązkom sprawozdawczym wobec Komisji (art. 63 ust. 2), co wydaje się być sprzeczne z ich niezależnością.

46. W związku z tym EROD i EIOD uważają, że przepisy te należy doprecyzować, aby były spójne z rozporządzeniem 2019/1020, EUDPR i RODO, a we wniosku należy jasno określić, że organy nadzorcze zgodnie z rozporządzeniem w sprawie sztucznej inteligencji muszą być całkowicie niezależne w wykonywaniu swoich zadań, ponieważ stanowiłoby to istotną gwarancję sprawowania właściwego nadzoru i egzekwowania przepisów przyszłego rozporządzenia.

47. EROD i EIOD pragną również przypomnieć, że organy ochrony danych (OOD) już teraz egzekwują przepisy RODO, EUDPR i LED w zakresie systemów sztucznej inteligencji wykorzystujących dane osobowe, aby zagwarantować ochronę praw podstawowych, a konkretnie prawa do ochrony danych. W związku z tym organy ochrony danych posiadają już w pewnym stopniu, zgodnie z wymogiem zawartym we wniosku dotyczącym krajowych organów nadzorczych, wiedzę na temat technologii dotyczących sztucznej inteligencji, danych i przetwarzania danych, praw podstawowych, a także wiedzę fachową w zakresie oceny zagrożeń dla praw podstawowych stwarzanych przez nowe technologie. Ponadto, gdy systemy sztucznej inteligencji opierają się na przetwarzaniu danych osobowych lub przetwarzają dane osobowe, przepisy zawarte we wniosku są bezpośrednio powiązane z ramami prawnymi dotyczącymi ochrony danych, co będzie miało miejsce w przypadku większości systemów sztucznej inteligencji objętych zakresem rozporządzenia. W rezultacie w ramach wniosku i organów ochrony danych nastąpi wzajemne powiązanie kompetencji organów nadzorczych.

48. W związku z tym wyznaczenie organów ochrony danych jako krajowych organów nadzorczych zapewniłoby bardziej zharmonizowane podejście regulacyjne i przyczyniłoby się do spójnej interpretacji przepisów dotyczących przetwarzania danych oraz uniknięcia sprzeczności w zakresie ich egzekwowania przez państwa członkowskie. Korzystne dla wszystkich zainteresowanych stron łańcucha wartości sztucznej inteligencji byłoby również posiadanie pojedynczego punktu kontaktowego odnośnie do wszystkich operacji przetwarzania danych osobowych objętych zakresem wniosku i ograniczenie kontaktów między dwoma różnymi organami regulacyjnymi w zakresie przetwarzania, którego dotyczy wniosek i przepisy RODO. W związku z tym EROD i EIOD uważają, że **organy ochrony danych powinny zostać wyznaczone jako krajowe organy nadzorcze zgodnie z art. 59 wniosku.**

49. W każdym razie, w zakresie, w jakim wniosek zawiera szczegółowe przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przyjęte na podstawie art. 16 TFUE, zgodność z tymi przepisami, zwłaszcza ograniczeniami stosowania systemów sztucznej inteligencji do zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa, **musi podlegać kontroli niezależnych organów**.

50. We wniosku nie zawarto jednak wyraźnego przepisu, który nadawałby uprawnienia w zakresie zapewnienia zgodności z tymi przepisami niezależnym organom. Jedyne odniesienie do właściwych organów nadzorczych odpowiedzialnych za ochronę danych na mocy przepisów RODO lub LED znajduje się w art. 63 ust. 5 wniosku, ale tylko jako do organów „nadzoru rynku" i zamiennie z niektórymi innymi organami. EROD i EIOD uważają, że taka sytuacja nie gwarantuje zgodności z wymogiem niezależnej kontroli określonym w art. 16 ust. 2 TFUE i art. 8 Karty.

2.5.2 Europejska Rada ds. Sztucznej Inteligencji

51. We wniosku ustanawia się „Europejską Radę ds. Sztucznej Inteligencji" (EAIB). EROD i EIOD uznają potrzebę spójnego i zharmonizowanego stosowania proponowanych ram, jak również zaangażowania niezależnych ekspertów w rozwój polityki UE w zakresie sztucznej inteligencji. Jednocześnie we wniosku przewiduje się przyznanie dominującej roli Komisji. W istocie Komisja nie tylko byłaby częścią EAIB, lecz również przewodniczyłaby jej i miałaby prawo weta przy przyjmowaniu regulaminu wewnętrznego EAIB. Kontrastuje to z potrzebą powołania europejskiego organu ds. sztucznej inteligencji niezależnego od jakichkolwiek wpływów politycznych. W związku z tym EROD i EIOD uważają, że przyszłe rozporządzenie w sprawie sztucznej inteligencji powinno zapewnić **EAIB większą autonomię**, aby rzeczywiście umożliwić jej zapewnienie spójnego stosowania rozporządzenia na całym jednolitym rynku.

52. EROD i EIOD zauważają również, że EAIB nie przyznano żadnych uprawnień w zakresie egzekwowania przepisów proponowanego rozporządzenia. Biorąc jednak pod uwagę rozpowszechnienie systemów sztucznej inteligencji na całym jednolitym rynku oraz prawdopodobieństwo wystąpienia przypadków transgranicznych, istnieje zasadnicza potrzeba zharmonizowanego egzekwowania przepisów oraz właściwego podziału kompetencji pomiędzy krajowymi organami nadzorczymi. EROD i EIOD zalecają zatem, aby mechanizmy współpracy między krajowymi organami nadzorczymi zostały określone w przyszłym rozporządzeniu w sprawie sztucznej inteligencji. EROD i EIOD proponują wprowadzenie mechanizmu gwarantującego ustanowienie pojedynczego punktu kontaktowego dla osób, których dotyczą przepisy, jak również dla przedsiębiorstw, w odniesieniu do każdego systemu sztucznej inteligencji, oraz organizacji, których działalność obejmuje ponad połowę państw członkowskich, EAIB może wyznaczyć organ krajowy, który będzie odpowiedzialny za egzekwowanie przepisów rozporządzenia w sprawie sztucznej inteligencji w odniesieniu do tego systemu sztucznej inteligencji.

53. Ponadto, biorąc pod uwagę niezależny charakter organów wchodzących w skład Rady, jest ona uprawniona do podejmowania działań z własnej inicjatywy, a nie tylko do udzielania Komisji porad i wsparcia. W związku z tym EROD i EIOD podkreślają potrzebę przedłużenia misji powierzonej Radzie, która ponadto nie odpowiada zadaniom wymienionym we wniosku.

54. Aby osiągnąć te cele, **EAIB powinna posiadać wystarczające i odpowiednie uprawnienia,** a jej status prawny powinien zostać doprecyzowany. W szczególności, aby zakres przedmiotowy przyszłego rozporządzenia pozostał aktualny, konieczne wydaje się zaangażowanie w jego rozwój organów odpowiedzialnych za jego stosowanie. W związku z tym EROD i EIOD zalecają, aby EAIB była uprawniona do proponowania Komisji zmian do załącznika I zawierających definicje technik i podejść w zakresie sztucznej inteligencji oraz załącznika III zawierających wykaz systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w art. 6 ust. 2. Komisja powinna również konsultować się z EAIB przed wprowadzeniem jakichkolwiek zmian do tych załączników.

55. W art. 57 ust. 4 wniosku przewiduje się wymianę informacji między Radą a innymi organami, jednostkami organizacyjnymi Unii i grupami doradczymi. Biorąc pod uwagę wcześniejsze prace w obszarze sztucznej inteligencji i wiedzę fachową w zakresie praw człowieka, EROD i EIOD zalecają rozważenie powołania Agencji Praw Podstawowych jako jednego z obserwatorów Rady.

3 ZWIĄZEK Z RAMAMI OCHRONY DANYCH

3.1 Związek wniosku z obowiązującymi unijnymi przepisami ochronie danych

56. Jasno określony związek między wnioskiem a obowiązującymi przepisami o ochronie danych jest podstawowym warunkiem wstępnym zapewnienia i utrzymania poszanowania i stosowania dorobku prawnego UE w dziedzinie ochrony danych osobowych. Takie prawo UE, w szczególności RODO, EUDPR i LED, należy uznać za warunek wstępny, na którym mogą opierać się dalsze wnioski ustawodawcze, nie naruszając obowiązujących przepisów ani nie ingerując w nie, w tym w odniesieniu do uprawnień organów nadzorczych i zarządzania.

57. Zdaniem EROD i EIOD ważne jest zatem, aby we wniosku wyraźnie uniknąć niespójności i ewentualnego konfliktu z przepisami RODO, EUDPR i LED. Nie tylko ze względu na pewność prawa, lecz również w celu uniknięcia sytuacji, w której wniosek skutkowałby bezpośrednim lub pośrednim zagrożeniem dla podstawowego prawa do ochrony danych osobowych, ustanowionego na mocy art. 16 TFUE i art. 8 Karty.

58. W szczególności samouczące się maszyny mogłyby chronić dane osobowe osób fizycznych tylko wtedy, gdyby zostało to tak zaprogramowane od samego początku. Niezbędna jest również natychmiastowa możliwość wykonania praw osób fizycznych na mocy art. 22 (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie) RODO lub art. 23 EUDPR, niezależnie od celów przetwarzania. W tym względzie inne prawa osób, których dane dotyczą, związane z prawem do usunięcia danych, prawem do korygowania danych zgodnie z przepisami o ochronie danych, należy zapewnić w

ramach systemów sztucznej inteligencji od samego początku, niezależnie od wybranego podejścia lub architektury technicznej w zakresie sztucznej inteligencji.

59. Wykorzystanie danych osobowych do uczenia systemów sztucznej inteligencji może prowadzić do generowania tendencyjnych wzorców decyzyjnych u podstaw systemu sztucznej inteligencji. Dlatego też należy wymagać zapewnienia różnych zabezpieczeń, w szczególności specjalistycznego nadzoru ze strony człowieka w takich procesach, aby zapewnić przestrzeganie i zagwarantowanie praw osób, których dane dotyczą, a także aby uniknąć wszelkich negatywnych skutków dla osób fizycznych. Właściwe organy powinny mieć również możliwość zaproponowania wytycznych w celu oceny stronniczości systemów sztucznej inteligencji i wspierania nadzoru ze strony człowieka.

60. Osoby, których dane dotyczą, należy zawsze informować, w przypadku gdy ich dane są wykorzystywane do celów szkolenia lub przewidywań w zakresie sztucznej inteligencji, o podstawie prawnej takiego przetwarzania, ogólnym wyjaśnieniu logiki (procedury) i zakresie działania systemu sztucznej inteligencji. W związku z tym w takich przypadkach zawsze należy zagwarantować osobom fizycznym prawo do ograniczenia przetwarzania (art. 18 RODO i art. 20 EUDPR), jak również prawo do usunięcia danych (art. 16 RODO i art. 19 EUDPR). Ponadto administrator danych powinien mieć wyraźny obowiązek informowania osoby, której dane dotyczą, o obowiązujących terminach zgłaszania sprzeciwu, ograniczenia, usunięcia danych itd. System sztucznej inteligencji musi być w stanie spełnić wszystkie wymogi w zakresie ochrony danych za pośrednictwem odpowiednich środków technicznych i organizacyjnych. Prawo do uzyskania wyjaśnienia powinno zapewniać dodatkową przejrzystość.

3.2 Piaskownica i dalsze przetwarzanie danych (art. 53 i 54 wniosku)

61. W ramach istniejących granic prawnych i moralnych ważne jest, aby promować innowacje europejskie za pośrednictwem narzędzi, takich jak piaskownica. Piaskownica daje możliwość zapewnienia zabezpieczeń niezbędnych do budowania zaufania i polegania na systemach sztucznej inteligencji. W złożonych środowiskach praktycy zajmujący się sztuczną inteligencją mogą mieć trudności z odpowiednim wyważeniem wszystkich interesów. Szczególnie w przypadku małych i średnich przedsiębiorstw o ograniczonych zasobach, funkcjonowanie w ramach piaskownicy regulacyjnej może przynieść szybszy wgląd w sytuację, a tym samym sprzyjać innowacjom.

62. Artykuł 53 ust. 3 wniosku stanowi, że piaskownica pozostaje bez wpływu na uprawnienia w zakresie nadzoru i stosowania środków naprawczych. Jeżeli to wyjaśnienie jest przydatne istnieje również potrzeba opracowania wskazówek lub wytycznych dotyczących tego, w jaki sposób osiągnąć odpowiednią równowagę między byciem organem nadzorczym z jednej strony, a udzielaniem szczegółowych wytycznych za pośrednictwem piaskownicy z drugiej strony.

63. Artykuł 53 ust. 6 stanowi, że zasady i warunki funkcjonowania piaskownic określa się w aktach wykonawczych. Ważne jest, aby opracować szczegółowe wytyczne w celu zapewnienia spójności i wsparcia przy tworzeniu i obsłudze piaskownic. Wiążące akty wykonawcze

mogłyby jednak ograniczyć zdolność każdego państwa członkowskiego do dostosowania piaskownicy do własnych potrzeb i lokalnych praktyk. W związku z tym EROD i EIOD zalecają, aby zamiast tego EAIB przedstawiła wytyczne dotyczące piaskownic.

64. Artykuł 54 wniosku ma na celu zapewnienie podstawy prawnej dalszego przetwarzania danych osobowych na potrzeby opracowywania określonych systemów sztucznej inteligencji w interesie publicznym w ramach piaskownicy regulacyjnej w zakresie sztucznej inteligencji. Niejasny pozostaje związek art. 54 ust. 1 wniosku z art. 54 ust. 2 i motywem 41 wniosku, a zatem również z obowiązującymi unijnymi przepisami o ochronie danych. Niemniej w RODO i EUDPR ustalono już podstawę „dalszego przetwarzania". Szczególnie w odniesieniu do przypadków, w których zezwolenie na dalsze przetwarzanie leży w interesie publicznym; równowaga między interesami administratora danych a interesami osoby, której dane dotyczą, nie musi utrudniać innowacji. Artykuł 54 wniosku nie odnosi się obecnie do dwóch ważnych kwestii: (i) w jakich okolicznościach, przy użyciu jakich (dodatkowych) kryteriów ważone są interesy osób, których dane dotyczą, oraz (ii) czy te systemy sztucznej inteligencji będą wykorzystywane wyłącznie w ramach piaskownicy. EROD i EIOD z zadowoleniem przyjmują wymóg dotyczący prawa Unii lub państwa członkowskiego w przypadku przetwarzania danych osobowych zgromadzonych zgodnie z LED w ramach piaskownicy, zalecają jednak dalsze doprecyzowanie tej kwestii, w sposób zgodny z przepisami RODO i EUDPR, głównie poprzez wyjaśnienie, że podstawa prawna takich piaskownic powinna być zgodna z wymogami ustanowionymi w art. 23 ust. 2 RODO i art. 25 EUDPR, oraz doprecyzowanie, że każde wykorzystanie piaskownicy musi zostać poddane gruntownej ocenie. Dotyczy to również pełnego wykazu warunków określonych w art. 54 ust. 1 lit. b)–j).

65. Pewne dodatkowe kwestie dotyczące ponownego wykorzystywania danych określone w art. 54 wniosku wskazują, że obsługa piaskownicy wymaga dużych zasobów i dlatego realistyczne jest oszacowanie, że tylko niewielka liczba przedsiębiorstw miałaby szansę na uczestnictwo. Uczestnictwo w piaskownicy może stanowić przewagę konkurencyjną. Umożliwienie ponownego wykorzystywania danych wymagałoby starannego rozważenia sposobu wyboru uczestników, tak aby dopilnować, by zostali oni objęci zakresem funkcjonowania piaskownicy i uniknąć niesprawiedliwego traktowania. EROD i EIOD obawiają się, że umożliwienie ponownego wykorzystywania danych w ramach piaskownicy odbiega od podejścia dotyczącego rozliczalności określonego w przepisach RODO, zgodnie z którymi rozliczalność spoczywa na administratorze danych, a nie na właściwym organie.

66. Ponadto EROD i EIOD uważają, że biorąc pod uwagę cele piaskownicy, które obejmują opracowywanie, testowanie i zatwierdzanie systemów sztucznej inteligencji, piaskownice nie mogą wchodzić w zakres LED. Choć w przepisach LED przewiduje się ponowne wykorzystanie danych do celów badań naukowych, dane przetwarzane w tym wtórnym celu będą podlegać przepisom RODO lub EUDPR, a nie LED.

67. Nie jest jasne, co będzie obejmowała piaskownica regulacyjna. Powstaje pytanie, czy proponowana piaskownica regulacyjna obejmuje infrastrukturę informatyczną w każdym państwie członkowskim z pewnymi dodatkowymi podstawami prawnymi dalszego przetwarzania, czy też zapewnia ona jedynie dostęp do wiedzy fachowej i wytycznych w

zakresie regulacji. EROD i EIOD wzywają prawodawcę do wyjaśnienia tej kwestii we wniosku oraz wyraźnego stwierdzenia we wniosku, że piaskownica regulacyjna nie pociąga za sobą obowiązku zapewnienia przez właściwe organy infrastruktury technicznej. W każdym przypadku właściwym organom należy zapewnić zasoby finansowe i ludzkie zgodnie z takim wyjaśnieniem.

68. Ponadto EROD i EIOD pragną położyć nacisk na rozwój transgranicznych systemów sztucznej inteligencji, które będą dostępne dla całego europejskiego jednolitego rynku cyfrowego. W przypadku takich systemów sztucznej inteligencji piaskownica regulacyjna jako narzędzie innowacji nie powinna stać się przeszkodą w rozwoju transgranicznym. W związku z tym EROD i EIOD zalecają przyjęcie skoordynowanego podejścia transgranicznego, które byłoby nadal wystarczająco dostępne na szczeblu krajowym dla wszystkich MŚP, a jednocześnie oferowałoby wspólne ramy w całej Europie, które nie byłyby zbyt restrykcyjne. Należy zachować równowagę między koordynacją na szczeblu europejskim a procedurami krajowymi, aby uniknąć kontrowersyjnego wdrażania przyszłego rozporządzenia w sprawie sztucznej inteligencji, które utrudniałoby innowacje w całej UE.

3.3 Przejrzystość

69. EROD i EIOD z zadowoleniem przyjmują fakt, że systemy sztucznej inteligencji wysokiego ryzyka są rejestrowane w publicznej bazie danych (o której mowa w art. 51 i 60 wniosku). Ta baza danych powinna być traktowana jako okazja do zapewnienia ogółowi społeczeństwa informacji na temat zakresu stosowania systemu sztucznej inteligencji oraz znanych wad i incydentów, które mogą zagrozić jego funkcjonowaniu, a także środków zaradczych przyjętych przez dostawców w celu zaradzenia im i ich naprawienia.

70. Kluczową zasadą demokracji jest stosowanie mechanizmów kontroli i równowagi. W związku z tym fakt, że obowiązek zachowania przejrzystości nie ma zastosowania do systemów sztucznej inteligencji wykorzystywanych do wykrywania przestępstw, zapobiegania im, prowadzenia dochodzeń w ich sprawie lub ich ścigania, stanowi zbyt szeroki wyjątek. Należy dokonać rozróżnienia między systemami sztucznej inteligencji, które są wykorzystywane do wykrywania przestępstw lub zapobiegania im, a systemami sztucznej inteligencji, których celem jest prowadzenie dochodzeń lub pomoc w ściganiu przestępstw. Zabezpieczenia w zakresie zapobiegania i wykrywania muszą być silniejsze ze względu na zasadę domniemania niewinności. Ponadto EROD i EIOD ubolewają nad brakiem we wniosku ostrzeżeń, które można interpretować jako zielone światło dla stosowania nawet niesprawdzonych systemów lub aplikacji opartych na sztucznej inteligencji wysokiego ryzyka.

71. W przypadkach, w których ze względu na konieczność zachowania tajemnicy, nawet w dobrze funkcjonującej demokracji, społeczeństwu można zapewnić przejrzystość jedynie w niewielkim stopniu, należy wprowadzić zabezpieczenia, a systemy sztucznej inteligencji powinny być rejestrowane przez właściwy organ nadzorczy i zapewniać mu przejrzystość.

72. Zapewnienie przejrzystości w systemach sztucznej inteligencji jest celem trudnym do osiągnięcia. W pełni ilościowe podejście decyzyjne przyjęte przez wiele systemów sztucznej inteligencji, z natury różniące się od podejścia ludzkiego polegającego głównie na rozumowaniu

przyczynowo-skutkowym i teoretycznym, może być sprzeczne z potrzebą uzyskania uprzedniego zrozumiałego wyjaśnienia wyników działania maszyny. W rozporządzeniu należy propagować nowe, bardziej proaktywne sposoby informowania w odpowiednim czasie użytkowników systemów sztucznej inteligencji o statusie (decyzyjnym) systemu w dowolnym momencie, zapewniając wczesne ostrzeganie o potencjalnych szkodliwych skutkach, tak aby osoby, których prawa i wolności mogą zostać naruszone w wyniku autonomicznych decyzji maszyny, mogły zareagować lub odwołać się od decyzji.

3.4 Przetwarzanie szczególnych kategorii danych i danych dotyczących przestępstw

73. Przetwarzanie szczególnych kategorii danych w dziedzinie egzekwowania prawa podlega przepisom unijnych ram ochrony danych, w tym przepisom LED, jak również ich wdrożeniu na szczeblu krajowym. Z wniosku wynika, że nie zapewnia on ogólnej podstawy prawnej przetwarzania danych osobowych, w tym szczególnych kategorii danych osobowych, por. motyw 41. Jednocześnie art. 10 ust. 5 wniosku stanowi, że „dostawcy takich systemów mogą przetwarzać szczególne kategorie danych osobowych". Ponadto zgodnie z tym samym przepisem należy zapewnić dodatkowe zabezpieczenia, wraz z przykładami. W związku z tym wydaje się, że wniosek koliduje ze stosowaniem przepisów RODO, LED i EUDPR. Choć EROD i EIOD z zadowoleniem przyjmują próbę zapewnienia odpowiednich zabezpieczeń, potrzebne jest bardziej spójne podejście regulacyjne, ponieważ obecne przepisy nie wydają się wystarczająco jasne, by stworzyć podstawę prawną przetwarzania szczególnych kategorii danych, i należy je uzupełnić o dodatkowe środki ochronne, które nadal wymagają oceny. Ponadto, jeżeli dane osobowe zostały zebrane w drodze przetwarzania w ramach LED, należy uwzględnić ewentualne dodatkowe zabezpieczenia i ograniczenia wynikające z krajowych transpozycji LED.

3.5 Mechanizmy zgodności

3.5.1 Certyfikacja

74. Jednym z głównych filarów wniosku jest certyfikacja. System certyfikacji przedstawiony we wniosku opiera się na strukturze podmiotów (organy notyfikujące/jednostki notyfikowane/Komisja) oraz mechanizmie oceny zgodności/certyfikacji obejmującym obowiązkowe wymogi mające zastosowanie do systemów sztucznej inteligencji wysokiego ryzyka, a także na europejskich normach zharmonizowanych na mocy rozporządzenia (UE) nr 1025/2012 i wspólnych specyfikacjach, które zostaną ustanowione przez Komisję. Mechanizm ten różni się od systemu certyfikacji mającego na celu zapewnienie zgodności z przepisami i zasadami w zakresie ochrony danych, przedstawionymi w art. 42 i 43 RODO. Nie jest jednak jasne, w jaki sposób certyfikaty wydane przez jednostki notyfikowane zgodnie z wnioskiem mogą współgrać z certyfikatami, znakami jakości i oznaczeniami w zakresie ochrony danych przewidzianymi w RODO, w przeciwieństwie do tego, co przewidziano w przypadku innych rodzajów certyfikatów (zob. art. 42 ust. 2 w odniesieniu do certyfikatów wydanych na mocy rozporządzenia (UE) 2019/881).

75. W zakresie, w jakim systemy sztucznej inteligencji wysokiego ryzyka opierają się na przetwarzaniu danych osobowych lub przetwarzają dane osobowe w celu realizacji swoich zadań, rozbieżności te mogą powodować niepewność prawa dla wszystkich zainteresowanych organów, ponieważ mogą prowadzić do sytuacji, w których systemy sztucznej inteligencji, certyfikowane zgodnie z wnioskiem i oznaczone oznakowaniem zgodności CE, po wprowadzeniu do obrotu lub oddaniu do użytku mogą być wykorzystywane w sposób niezgodny z przepisami i zasadami w zakresie ochrony danych.

76. We wniosku brakuje wyraźnego związku z przepisami o ochronie danych oraz innymi przepisami Unii i państw członkowskich mającymi zastosowanie do każdego „obszaru" systemu sztucznej inteligencji wysokiego ryzyka wymienionego w załączniku III. W szczególności wniosek powinien uwzględniać zasady minimalizacji danych i ochrony danych w fazie projektowania jako jeden z aspektów, które należy wziąć pod uwagę przed uzyskaniem oznakowania zgodności CE, z uwagi na możliwy wysoki poziom ingerencji systemów sztucznej inteligencji wysokiego ryzyka w podstawowe prawa do prywatności i ochrony danych osobowych oraz potrzebę zapewnienia wysokiego poziomu zaufania do systemu sztucznej inteligencji. W związku z tym EROD i EIOD zalecają zmianę wniosku w celu wyjaśnienia związku między certyfikatami wydawanymi na mocy wspomnianego rozporządzenia a certyfikatami, znakami jakości i oznaczeniami w zakresie ochrony danych. Ponadto organy ochrony danych powinny być zaangażowane w przygotowanie i ustanowienie zharmonizowanych norm i wspólnych specyfikacji.

77. W związku z art. 43 wniosku, dotyczącym oceny zgodności, odstępstwo od procedury oceny zgodności określone w art. 47 wydaje się szczególnie szerokie i obejmuje zbyt wiele wyjątków, takich jak nadzwyczajne względy dotyczące bezpieczeństwa publicznego lub ochrony życia i zdrowia osób fizycznych, ochrony środowiska oraz ochrony kluczowych aktywów przemysłowych i infrastrukturalnych. Proponujemy, aby prawodawcy zawęzili ich zakres.

3.5.2 Kodeksy postępowania

78. Zgodnie z art. 69 wniosku Komisja i państwa członkowskie zachęcają do sporządzania i ułatwiają sporządzanie kodeksów postępowania mających na celu wspieranie dobrowolnego stosowania przez dostawców systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem wymogów mających zastosowanie do systemów sztucznej inteligencji wysokiego ryzyka, a także wymogów dodatkowych. Zgodnie z motywem 78 RODO EROD i EIOD zalecają zidentyfikowanie i określenie synergii między tymi instrumentami a kodeksami postępowania przewidzianymi w RODO, które wspierają zgodność z przepisami o ochronie danych. W tym kontekście należy wyjaśnić, czy ochrona danych osobowych ma być uważana za jeden z „dodatkowych wymogów", które mogą być uwzględnione w kodeksach postępowania, o których mowa w art. 69 ust. 2. Istotne jest również zapewnienie, aby „specyfikacje i rozwiązania techniczne" określone w kodeksach postępowania, o których mowa w art. 69 ust. 1, mające na celu wspieranie zgodności z wymogami projektu rozporządzenia w sprawie sztucznej inteligencji, nie były sprzeczne z przepisami i zasadami przewidzianymi w RODO i EUDPR. Dzięki temu korzystanie z tych narzędzi przez dostawców systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem – o ile systemy te opierają się na przetwarzaniu danych

osobowych lub przetwarzają dane osobowe w celu realizacji swoich zadań – stanowiłoby wartość dodaną, ponieważ zagwarantuje to, że administratorzy i podmioty przetwarzające będą w stanie wypełnić swoje obowiązki w zakresie ochrony danych dzięki korzystaniu z tych systemów.

79. Jednocześnie ramy prawne godnego zaufania systemu sztucznej inteligencji zostałyby uzupełnione dzięki integracji kodeksów postępowania w celu zwiększenia zaufania do korzystania z tej technologii w sposób bezpieczny i zgodny z prawem, w tym z poszanowaniem praw podstawowych. Należy jednak wzmocnić konstrukcję tych instrumentów, przewidując mechanizmy mające na celu sprawdzenie, czy kodeksy te zawierają skuteczne „specyfikacje i rozwiązania techniczne" oraz „jasno określone cele i kluczowe wskaźniki skuteczności działania służące do pomiaru stopnia realizacji tych celów" jako integralne części przedmiotowych kodeksów. Ponadto brak jakiegokolwiek odniesienia do (obowiązkowych) mechanizmów monitorowania kodeksów postępowania mających na celu sprawdzenie, czy dostawcy systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem przestrzegają ich postanowień, a także możliwość sporządzania (i samodzielnego wdrażania) wspomnianych kodeksów przez poszczególnych dostawców (zob. pkt 5.2.7 uzasadnienia) może dodatkowo osłabić skuteczność i wykonalność tych instrumentów.

80. Ponadto EROD i EIOD zwracają się z wnioskiem o przedstawienie wyjaśnień dotyczących różnych rodzajów inicjatyw, które Komisja może opracować, zgodnie z motywem 81 wniosku, „aby ułatwiać zmniejszenie barier technicznych utrudniających transgraniczną wymianę danych na potrzeby rozwoju sztucznej inteligencji".

4 WNIOSKI

81. Mimo że EROD i EIOD z zadowoleniem przyjmują wniosek Komisji i uważają, że takie rozporządzenie jest niezbędne do zagwarantowania praw podstawowych obywateli i mieszkańców UE, uważają, że wniosek wymaga dostosowania w kilku kwestiach, aby zapewnić jego stosowanie i skuteczność.

82. Biorąc pod uwagę złożony charakter wniosku, jak również kwestie, które ma on rozwiązać, pozostaje jeszcze wiele do zrobienia, zanim wniosek umożliwi wprowadzenie dobrze funkcjonujących ram prawnych, skutecznie uzupełniających przepisy RODO w zakresie ochrony podstawowych praw człowieka i jednocześnie wspierających innowacje. EROD i EIOD nadal będą oferować swoje wsparcie w tych dążeniach.

Bruksela, 18 czerwca 2021 r.

W imieniu Europejskiej Rady Ochrony Danych	W imieniu Europejskiego Inspektora Ochrony Danych
Przewodnicząca	Inspektor
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI