

Bruksela, 12 września 2022 r.
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

Międzyinstytucjonalny numer
referencyjny:
2021/0106(COD)

OPINIA SŁUŻBY PRAWNEJ¹

Od:	Służba Prawna
Dotyczy:	Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji – Adekwatność art. 114 i 16 TFUE jako podstaw prawnych w kontekście przepisów mających zastosowanie do organów ścigania i organów sądowych

I. WPROWADZENIE

1. W proponowanym rozporządzeniu ustanowiono zharmonizowane przepisy dotyczące wprowadzania do obrotu i oddawania do użytku systemów sztucznej inteligencji w Unii („proponowane rozporządzenie”)².

¹ Niniejszy dokument zawiera opinię prawną, która podlega ochronie na mocy art. 4 ust. 2 rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji; opinii tej Rada Unii Europejskiej nie podaje do wiadomości publicznej. Rada zastrzega sobie możliwość dochodzenia wszelkich praw, jeżeli opinia ta zostanie w sposób nieuprawniony opublikowana.

² Dok. 8115/21.

2. Na posiedzeniu Grupy Roboczej ds. Telekomunikacji i Społeczeństwa Informacyjnego, które odbyło się w dniu 7 kwietnia 2022 r., Służba Prawna Rady („Służba Prawna”) zabrała głos w kwestii adekwatności podwójnej podstawy prawnej (art. 16 i 114 TFUE) proponowanego rozporządzenia dotyczącego systemów sztucznej inteligencji. Potwierdziła, że art. 16 i 114 TFUE stanowią prawidłowe podstawy prawne wniosku i że odniesienie do art. 87 ust. 2 TFUE – zamiast do art. 114 TFUE – nie jest właściwe. Niniejsza opinia, sporządzona na wniosek wspomnianej grupy roboczej, zawiera zapis i rozwinięcie wyjaśnień przekazanych przez przedstawiciela Służby Prawnej podczas posiedzenia.
3. Systemy sztucznej inteligencji zdefiniowano w art. 3 pkt 1 proponowanego rozporządzenia. Ogólnie rzecz biorąc, odpowiadają one pewnym rodzajom oprogramowania. Proponowane rozporządzenie ma zastosowanie zarówno do dostawców wprowadzających systemy sztucznej inteligencji do obrotu, jak i do dostawców oddających takie systemy do użytku. Ponadto proponowane rozporządzenie ma również zastosowanie do użytkowników. Dostawcą może być osoba fizyczna lub prawna lub organ publiczny lub podmiot, które opracowują system sztucznej inteligencji lub zlecają jego opracowanie w celu wprowadzenia go do obrotu lub oddania go do użytku pod własną nazwą handlową lub własnym znakiem towarowym. Użytkownikiem może być osoba fizyczna lub prawna, organ publiczny, agencja lub inny podmiot, które korzystają z systemu sztucznej inteligencji pod swoją kontrolą.

4. Zgodnie z definicjami zawartymi w art. 3 organy ścigania i organy sądowe mogą kwalifikować się jako dostawcy lub użytkownicy systemu sztucznej inteligencji. Systemy sztucznej inteligencji, których przeznaczeniem określonym przez dostawcę jest egzekwowanie prawa lub sprawowanie wymiaru sprawiedliwości, zostały sklasyfikowane w załączniku III jako systemy wysokiego ryzyka. Jako takie podlegają one podstawowym wymogom (zarządzanie ryzykiem, testowanie, zarządzanie danymi, dokumentacja techniczna, przejrzystość, nadzór ze strony człowieka, dokładność, solidność i cyberbezpieczeństwo) i obowiązkom (takim jak systemy zarządzania jakością, dokumentacja techniczna, ocena zgodności, działania naprawcze, obowiązek informowania, obowiązki importerów i dystrybutorów), jak również normom i ocenie zgodności. Te zharmonizowane przepisy są wzorowane na przepisach regulujących bezpieczeństwo produktów i ustanowionych w dyrektywie 2006/42/WE (maszyny)³ i w rozporządzeniu 2017/745 (wyroby medyczne)⁴.
5. Jeśli chodzi o systemy sztucznej inteligencji wykorzystujące systemy zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa, należą one do kategorii zakazanych systemów sztucznej inteligencji. Od tego zakazu stosowania systemów sztucznej inteligencji istnieją jednak wyjątki. W rzeczy samej, państwa członkowskie mogą dopuścić możliwość stosowania takich systemów. W takim przypadku systemy te podlegają szczegółowym ograniczeniom i zabezpieczeniom, tak by ich stosowanie nie wykraczało poza to, co jest absolutnie niezbędne, i by chronić podstawowe prawo do ochrony danych osobowych. Te ograniczenia i zabezpieczenia są przewidziane w proponowanym rozporządzeniu na podstawie art. 16 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”) i muszą zostać uzupełnione prawem krajowym. Art. 5 ust. 1 lit. d) i art. 5 ust. 2, 3 i 4 proponowanego rozporządzenia stanowią *lex specialis* w stosunku do dyrektywy 2016/680 (dyrektywa o ochronie danych w sprawach karnych), która została przyjęta na podstawie art. 16 ust. 2 TFUE.

³ Dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE, Dz.U. L 157 z 9.6.2006, s. 24–86.

⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylecia dyrektyw Rady 90/385/EWG i 93/42/EWG, Dz.U. L 117 z 5.5.2017, s. 1–175.

Zgodnie z art. 5 ust. 1 lit. d) cele tych systemów ograniczają się do:

- i) ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci;
- ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu;
- iii) wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub osoby podejrzanej o popełnienie przestępstwa, o którym mowa w art. 2 ust. 2 decyzji o europejskim nakazie aresztowania⁵ 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.

Zgodnie z art. 5 ust. 3 wykorzystywanie takich technologii przez organy ścigania wymaga uzyskania uprzedniego zezwolenia od organu sądowego lub administracyjnego. W należycie uzasadnionych nagłych przypadkach można jednak rozpocząć wykorzystywanie systemu bez zezwolenia, a o zezwolenie można wystąpić w trakcie lub po zakończeniu wykorzystywania.

Zgodnie z art. 5 ust. 4 państwo członkowskie może podjąć decyzję o zezwoleniu na wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa i ustanowić niezbędne szczegółowe przepisy dotyczące zarówno wniosków o uprzednie zezwolenia, wydawania tych zezwoleń i ich wykonywania, jak i powiązanych przestępstw.

6. Podstawami prawnymi proponowanego rozporządzenia są art. 16 TFUE (ochrona danych osobowych) i art. 114 TFUE (funkcjonowanie rynku wewnętrznego). W związku z tym pojawia się pytanie o to, czy są to adekwatne podstawy prawne w odniesieniu do zharmonizowanych przepisów mających zastosowanie do systemów sztucznej inteligencji udostępnianych lub wykorzystywanych przez organy ścigania i organy sądowe.

⁵ 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.

7. W niniejszej opinii skoncentrowano się przede wszystkim na kwestii, czy art. 114 TFUE jest adekwatną podstawą prawną w szczególnym kontekście organów ścigania, o których mowa w szeregu przepisów proponowanego rozporządzenia, tj. w odniesieniu do systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej oraz systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 6. W związku z tym rozważono w niej to, czy zamiast art. 114 TFUE nie należałoby zastosować art. 87 ust. 2 TFUE (współpraca policyjna) jako podstawy prawnej udostępniania i wykorzystywania systemów sztucznej inteligencji przez organy ścigania (część II). W analogiczny sposób, wniosek podsumowujący niniejszą notę można zastosować do organów sądowych, o których mowa w załączniku III dotyczącym systemów sztucznej inteligencji wysokiego ryzyka.
8. W niniejszej notce rozważono również to, czy art. 16 TFUE jest adekwatną dodatkową podstawą prawną i czy należy stosować protokoły nr 21 i 22 w kontekście wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej przez organy ścigania (część III).

II. ADEKWATNOŚĆ ART. 114 TFUE JAKO PODSTAWY PRAWNEJ

9. Zgodnie z utrwalonym orzecznictwem wybór podstawy prawnej aktu Unii nie zależy od tego, na czym – zdaniem danej instytucji – polega realizowany cel, lecz musi zostać dokonany na podstawie obiektywnych kryteriów mogących podlegać kontroli sądowej, w tym w szczególności na podstawie celu i treści danego aktu. Jeżeli analiza danego aktu wykaże, że wyznaczono mu dwa cele lub że ma on dwa elementy składowe i jeden z tych celów lub elementów składowych można zidentyfikować jako główny lub dominujący, podczas gdy drugi jest jedynie pomocniczy, wówczas ten akt należy wydać na jednej podstawie prawnej, tj. na tej podstawie, która wymagana jest z racji głównego lub dominującego celu lub elementu składowego. Jedynie w wyjątkowych przypadkach, jeżeli zostanie ustalone, że dany akt dąży jednocześnie do realizacji większej liczby celów, które są ze sobą nierozzerwalnie związane, przy czym żaden z nich nie jest drugorzędny ani pośredni w stosunku do drugiego, wówczas taki akt można wydać na różnych, odpowiadających poszczególnym celom podstawach prawnych, chyba że procedury przewidziane w każdej z tych podstaw prawnych są ze sobą niezgodne. Należy również zauważyć, że w art. 114 ust. 1 zdanie pierwsze TFUE stwierdza się wyraźnie, iż postanowienia tego artykułu mają zastosowanie „[z] zastrzeżeniem, że Traktaty nie stanowią inaczej”. W związku z tym zastosowanie art. 114 TFUE jest uzasadnione jedynie wówczas, gdy podstawy prawnej przyjęcia danego aktu nie może stanowić żadne inne bardziej szczegółowe postanowienie⁶. Jeżeli Traktat zawiera bardziej szczegółowe postanowienie mogące stanowić podstawę prawną danego aktu, podstawę tego aktu musi stanowić to postanowienie⁷.

⁶ Opinia Służby Prawnej z dnia 17 maja 2016 r., 9007/16, pkt 6.

⁷ Wyrok z dnia 29 kwietnia 2004 r., *Komisja przeciwko Radzie*, C-338/01, EU:C:2004:253, pkt 60.

A. CEL PROPONOWANEGO ROZPORZĄDZENIA

10. W proponowanym rozporządzeniu harmonizuje się wprowadzanie do obrotu, oddawanie do użytku i wykorzystywanie określonego rodzaju oprogramowania (systemów sztucznej inteligencji). Fakt, że organy publiczne i operatorzy prywatni mogą być dostawcami lub użytkownikami takich systemów sztucznej inteligencji nie jest sam w sobie niezgodny z podstawą prawną, jaką jest art. 114 TFUE⁸.
11. Ponadto fakt, że organy ścigania lub podmioty działające w ich imieniu mogą być dostawcami lub użytkownikami takich systemów sztucznej inteligencji, nie wystarcza, aby uzasadnić odniesienie do podstawy prawnej, jaką jest art. 87 TFUE. Aby stwierdzić, czy odniesienie takie jest konieczne, należy przeanalizować cel i treść proponowanego rozporządzenia.
12. Ogólnym celem proponowanego rozporządzenia jest – także w odniesieniu do systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej oraz systemów sztucznej inteligencji wysokiego ryzyka – zapewnienie spójnego i wysokiego poziomu ochrony w całej Unii, a jednocześnie zapobieganie rozbieżnościom utrudniającym swobodny obrót systemami sztucznej inteligencji oraz powiązanymi produktami i usługami na rynku wewnętrznym. Ustanawia się w nim jednolite obowiązki operatorów i gwarantuje jednolitą ochronę nadrzędnego interesu publicznego i praw osób na całym rynku wewnętrznym (motyw 2). W szczególności ustanawia się w nim przepisy regulujące wprowadzanie do obrotu i oddawanie do użytku niektórych systemów sztucznej inteligencji, zapewniając w ten sposób sprawne funkcjonowanie rynku wewnętrznego i umożliwiając swobodny obrót tymi systemami zgodnie z zasadą swobodnego przepływu towarów i usług (motyw 5). W ogólnym ujęciu celem wniosku jest ustanowienie wiarygodnej sztucznej inteligencji już w fazie projektowania, mającej zastosowanie we wszystkich dziedzinach, wraz z pełnym zestawem przepisów dotyczących opracowywania, wprowadzania do obrotu i wykorzystywania produktów, usług i systemów opartych na sztucznej inteligencji. Ze względu na to, że wiele usług i produktów już wykorzystuje sztuczną inteligencję i tendencja ta będzie nadal rozwijać się w przyszłości, we wniosku ustanowiono – zgodnie z logiką rynku wewnętrznego – „ramy bezpieczeństwa produktów” oparte na zestawie czterech kategorii ryzyka. Przewidziano w nim wymogi dotyczące wejścia na rynek i certyfikacji systemów sztucznej inteligencji wysokiego ryzyka, wprowadzając obowiązkową procedurę oznakowania zgodności CE.

⁸ Zob. opinia Służby Prawnej (ST 11395/14 pkt 39–41) i precedensy, takie jak dyrektywa (UE) 2016/2102 oraz dyrektywy 2014/24/UE, 2014/25/UE i 2014/23/UE.

13. Żaden z deklarowanych celów proponowanego rozporządzenia nie odnosi się do zapewniania bezpieczeństwa publicznego. Nawet jeśli cele dotyczące bezpieczeństwa publicznego mają zostać osiągnięte pośrednio poprzez harmonizację wprowadzania do obrotu / oddawania do użytku / wykorzystywania systemów sztucznej inteligencji przez organy ścigania, Trybunał⁹, dokonując wykładni art. 87 ust. 2 TFUE w świetle art. 67 TFUE, orzekł, że jeśli artykuł ten ma być podstawą aktu Unii, akt ten, z uwzględnieniem jego celu i treści, musi łączyć się bezpośrednio z celami określonymi w art. 67 TFUE (tj., w przytoczonej sprawie, zapobieganiem przestępczości i współpracą policyjną). Jest to wykluczone w kontekście proponowanego rozporządzenia, ponieważ jedynymi zharmonizowanymi przepisami dotyczącymi korzystania z takich systemów przez organy ścigania są (1) przepisy zbliżone do przepisów dotyczących bezpieczeństwa produktów, mające jednolite zastosowanie do wszystkich dostawców i użytkowników w kontekście wprowadzania do obrotu /oddawania do użytku lub wykorzystywania systemów sztucznej inteligencji lub (2) przepisy dotyczące ochrony danych osobowych, w odniesieniu do których dodano podstawę prawną w postaci art. 16 TFUE (zob. część III poniżej).
14. W innej sprawie¹⁰, pomimo tego, że celem zmiany dyrektywy o broni palnej było zapewnienie wyższego poziomu bezpieczeństwa publicznego w związku z zagrożeniem terrorystycznym i innymi formami przestępczości, Trybunał orzekł, że harmonizacja aspektów związanych z bezpieczeństwem towarów jest jednym z zasadniczych elementów służących zapewnieniu właściwego funkcjonowania rynku wewnętrznego, ponieważ rozbieżne przepisy w tej dziedzinie mogą skutkować barierami w handlu¹¹.

⁹ Wyrok z dnia 6 maja 2014 r., *Komisja Europejska przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej*, C-43/12, EU:C:2014:298.

¹⁰ Wyrok z dnia 3 grudnia 2019 r., *Republika Czeska przeciwko Parlamentowi Europejskiemu*, C-482/17, EU:C:2019:1035.

¹¹ Tamże, pkt 57: „Specyfika broni palnej polega zaś, wbrew temu, co twierdzi Rzeczpospolita Polska, na tym, że jest ona niebezpieczna nie tylko dla użytkownika, lecz także dla ogółu ludności, jak już Trybunał zdążył stwierdzić w pkt 54 wyroku z dnia 23 stycznia 2018 r., *Buhagiar i in.* (C- 267/16, EU:C:2018:26), toteż względy bezpieczeństwa publicznego są, jak przypomniano w motywie piątym dyrektywy 91/477, niezbędnym elementem uregulowań dotyczących nabywania i posiadania tych towarów”. Zob. też wyrok z dnia 23 stycznia 2018 r., *Albert Buhagiar i in. przeciwko Minister for Justice*, C-267/16, EU:C:2018:26, pkt 54: „W tym względzie należy wskazać, że z uwagi na ryzyko dla bezpieczeństwa osób, jakie stanowi broń palna, jej swobodny obrót mógł zostać osiągnięty jedynie poprzez ścisłe ramy warunków jej transferu między państwami członkowskimi, obejmujące zasadę uprzedniego zezwolenia wydanego przez państwa członkowskie, których dotyczy transfer danych towarów”.

15. Cele proponowanego rozporządzenia – w tym przepisów art. 5 ust. 1 lit. d) i art. 5 ust. 2, 3 i 4 dotyczących wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa oraz przepisów regulujących systemy sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 6 – nie łączą się bezpośrednio z celem dotyczącym bezpieczeństwa publicznego. Wprost przeciwnie – wniosek stanowi odpowiedź na główne obawy związane z tym, jak systemy sztucznej inteligencji wpływają na zdrowie, bezpieczeństwo i prawa podstawowe. W związku z tym odpowiednie przepisy łączą się bezpośrednio z celem dotyczącym zapewnienia równych warunków działania w zakresie wprowadzania do obrotu / oddawania do użytku lub wykorzystywania systemów sztucznej inteligencji na rynku wewnętrznym, a jednocześnie celem dotyczącym chronienia zdrowia, bezpieczeństwa i praw podstawowych użytkowników.
16. W świetle powyższego głównym celem proponowanego rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego w rozumieniu art. 114 TFUE, a cele, o których mowa w art. 67 TFUE, łączą się tylko pośrednio i uzupełniająco z tym głównym celem.

B. TREŚĆ PROPONOWANEGO ROZPORZĄDZENIA

17. Proponowane rozporządzenie zawiera przede wszystkim przepisy dotyczące tego, co jest konieczne do wprowadzenia do obrotu (lub oddania do użytku) konkretnego produktu (oprogramowania w zakresie sztucznej inteligencji), tak by był on bezpieczny i zapewniał poszanowanie praw podstawowych. W proponowanym rozporządzeniu ustanowiono pełny zestaw przepisów dotyczących opracowywania, wprowadzania do obrotu i wykorzystywania produktów, usług i systemów opartych na sztucznej inteligencji. Nie zobowiązuje się w nim organów ścigania do wykorzystywania systemów sztucznej inteligencji, które zgodnie z prawem zostały wprowadzone do obrotu, ani nie reguluje bezpośrednio sposobu, w jaki organy ścigania powinny takie systemy wykorzystywać. Zamiast tego wyraźnie określa się sytuacje, w których dane przeznaczenie jest uznawane za przeznaczenie wysokiego ryzyka dlatego, że system sztucznej inteligencji będzie wykorzystywany przez organy ścigania lub organy sądowe.

18. Co prawda art. 29 proponowanego rozporządzenia zawiera przepisy dotyczące warunków wykorzystywania systemów sztucznej inteligencji wysokiego ryzyka, ale uregulowanie to nie ogranicza się tylko do tego sektora, ma ograniczony zakres (chodzi głównie o instrukcje obsługi produktu) i jest nierozdzielnie związane z obowiązkami twórców systemów sztucznej inteligencji wynikającymi z proponowanego rozporządzenia. Ponadto zapewniono w nim państwom członkowskim pewną swobodę w zakresie ustanawiania dalszych przepisów dotyczących wykorzystywania takich systemów sztucznej inteligencji wysokiego ryzyka. Jeśli chodzi o systemy zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa (art. 5), w proponowanym rozporządzeniu częściowo reguluje się wykorzystywanie takich systemów w kontekście ochrony przewidzianej w art. 16 TFUE (zob. część III poniżej).
19. Co więcej, wyłącznie państwa członkowskie mogą zdecydować o wprowadzeniu przepisów, które umożliwią pełne lub częściowe zezwolenie na wykorzystywanie takich systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym”. Szczegółowe warunki takiego wykorzystywania należy określić w prawie krajowym, ale muszą one być zgodne z ogólnymi kryteriami i zabezpieczeniami określonymi w rozporządzeniu, takimi jak: uprzednie zezwolenie organu sądowego lub administracyjnego, wnioski o uprzednie zezwolenie, wydanie i wykonanie takiego zezwolenia, jak również wskazanie przestępstw, w przypadku których można korzystać z takich systemów.

20. Systemy sztucznej inteligencji są szczególnym rodzajem oprogramowania. Zharmonizowane przepisy mające zastosowanie do wprowadzania do obrotu lub oddawania do użytku / wykorzystywania systemów sztucznej inteligencji są zatem zharmonizowanymi przepisami zbliżonymi do przepisów dotyczących bezpieczeństwa produktów. Stosuje się je w jednolity sposób bez rozróżniania między użytkownikami publicznymi i prywatnymi. Zgodnie z odpowiednimi motywami proponowanego rozporządzenia należy zatem zapewnić spójny i wysoki poziom ochrony w całej Unii. Jednocześnie należy zapobiegać rozbieżnościom utrudniającym swobodny obrót systemami sztucznej inteligencji oraz powiązanymi produktami i usługami na rynku wewnętrznym. W tym celu w rozporządzeniu ustanawia się na podstawie art. 114 TFUE jednolite obowiązki operatorów i gwarantuje jednolitą ochronę nadrzędnego interesu publicznego i praw osób na całym rynku wewnętrznym¹².
21. Proponowane rozporządzenie zawiera szereg odniesień do egzekwowania prawa, zarządzania kontrolą graniczną i sprawowania wymiaru sprawiedliwości; odniesienia te zamieszczono w załączniku III dotyczącym systemów sztucznej inteligencji wysokiego ryzyka (odpowiednio pkt 6, 7 i 8). Obejmują one szczegółowe i wyczerpujące wyliczenie systemów odpowiadające art. 6 ust. 2, które uzupełnia inne systemy wysokiego ryzyka w odniesieniu do zagrożeń dla bezpieczeństwa produktów, o których mowa w art. 6 ust. 1. W rzeczy samej, zgodnie z art. 6 ust. 1, niektóre systemy sztucznej inteligencji należy z definicji uznać za systemy wysokiego ryzyka ze względu na skalę szkód, które mogą spowodować, i wysokie ryzyko dla praw podstawowych, zdrowia i bezpieczeństwa. Inne systemy, które uznano za systemy wysokiego ryzyka i wymieniono w załączniku III, dotyczą takich obszarów jak: edukacja, zarządzanie infrastrukturą krytyczną, zatrudnienie, identyfikacja biometryczna i kategoryzacja, a także dostęp do podstawowych usług publicznych i prywatnych.

¹² Unijne ramy prawne określające zharmonizowane przepisy dotyczące sztucznej inteligencji są zatem niezbędne do wspierania rozwoju, wykorzystywania i upowszechniania sztucznej inteligencji na rynku wewnętrznym, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony interesów publicznych, takich jak zdrowie i bezpieczeństwo oraz ochrona praw podstawowych, uznanych i chronionych przez prawo Unii. Aby osiągnąć ten cel, należy ustanowić przepisy regulujące wprowadzanie do obrotu i oddawanie do użytku niektórych systemów sztucznej inteligencji, zapewniając w ten sposób sprawne funkcjonowanie rynku wewnętrznego i umożliwiając swobodny obrót tymi systemami zgodnie z zasadą swobodnego przepływu towarów i usług (zob. motywy 2 i 5 wniosku).

22. Przedmiotowe przepisy dotyczące systemów sztucznej inteligencji wysokiego ryzyka nie rozstrzygają jednak tego, czy z systemów tych powinny korzystać organy ścigania i organy sądowe (lub organy w innych wymienionych obszarach). Proponowane rozporządzenie będzie miało jedynie pośredni wpływ na faktyczny rozwój systemów sztucznej inteligencji, które mogą być wykorzystywane przez organy ścigania, i na systemy sztucznej inteligencji wykorzystywane obecnie i w przyszłości. W związku z tym przepisy te odnoszą się do systemów sztucznej inteligencji, które są „przeznaczone do wykorzystywania” przez takie organy (zob. np. art. 3 ust. 12, art. 8 ust. 2 i załącznik III). Konsekwencją uznania danego systemu sztucznej inteligencji za system wysokiego ryzyka jest stosowanie szczególnego zestawu przepisów dotyczących zarządzania ryzykiem, zarządzania danymi i specyfikacji technicznych. Użytkownicy takich systemów sztucznej inteligencji wysokiego ryzyka muszą przestrzegać instrukcji obsługi, przechowywać rejestry zdarzeń i przeprowadzać oceny skutków dla ochrony danych.
23. Ponadto obowiązki użytkownika inne niż obowiązki wynikające z instrukcji obsługi mogą zostać określone w prawie unijnym lub krajowym, bez uszczerbku dla przysługującej użytkownikowi swobody organizowania jego zasobów własnych i działań w celu wdrożenia wskazanych przez dostawcę środków nadzoru ze strony człowieka (art. 29 ust. 2 proponowanego rozporządzenia). Przepisy te przewidują wprowadzenie kolejnych zabezpieczeń chroniących prawa podstawowe w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka.

24. W świetle powyższego należy podkreślić, że proponowane rozporządzenie nie zawiera przepisów, które mają umożliwić lub uniemożliwić organom ścigania wykorzystywanie systemu sztucznej inteligencji wysokiego ryzyka wprowadzonego do obrotu. Na mocy proponowanych przepisów do systemu sztucznej inteligencji opracowanego lub wykorzystywanego przez organy ścigania będzie stosowana odrębna klasyfikacja (system wysokiego ryzyka) uwzględniająca zamierzone wykorzystanie danego systemu. Takie wykorzystywanie podlegałoby prawu krajowemu i w określonym zakresie zależałoby od samych organów ścigania. Proponowane rozporządzenie ustanawia w art. 29 minimalne warunki wykorzystywania (dotyczące tylko instrukcji obsługi) w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka, w tym systemów wymienionych w załączniku III pkt 6, 7 i 8, które to warunki zostaną uzupełnione przepisami prawa krajowego. Zgodnie z orzecznictwem Trybunału należy zatem dokonać rozróżnienia między, z jednej strony, zamierzonym celem proponowanego rozporządzenia, którym nie jest uregulowanie wykorzystywania systemów sztucznej inteligencji przez organy ścigania, a, z drugiej strony, skutkami, które rozporządzenie to może pośrednio powodować¹³ i które nie mają znaczenia dla analizy adekwatności podstawy prawnej.
25. Systemy wymienione w pkt 6, 7 i 8 (dotyczących odpowiednio egzekwowania prawa, migracji i sprawowania wymiaru sprawiedliwości) nie przeważają wśród systemów sztucznej inteligencji wysokiego ryzyka. W rzeczy samej, zgodnie z proponowanym rozporządzeniem system sztucznej inteligencji wysokiego ryzyka niekoniecznie musi być jednym z systemów wymienionych w załączniku III. Większość systemów wysokiego ryzyka to bowiem systemy wymienione w sposób ogólny w art. 6 ust. 1 lit. a) i b) proponowanego rozporządzenia (w związku z bezpieczeństwem produktów). Inne systemy sztucznej inteligencji wysokiego ryzyka są wyszczególnione w załączniku III obejmującym punkty 1 (identyfikacja biometryczna), 2 (infrastruktura krytyczna), 3 (kształcenie i szkolenie zawodowe) i 4 (zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia), które odnoszą się do obszarów innych niż wymiar sprawiedliwości i sprawy wewnętrzne („WSiSW”). Wszyscy użytkownicy takich systemów sztucznej inteligencji wysokiego ryzyka podlegają ustanowionemu jednolitemu systemowi nie ze względu na ich szczególny status (np. na to, czy jest to podmiot gospodarczy czy organ publiczny), ale z uwagi na ochronę zdrowia, bezpieczeństwa i praw podstawowych.

¹³ Zob. wyrok Trybunału z dnia 21 czerwca 2018 r., *Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej*, C-5/16, EU:C:2018:483, pkt 63–68, oraz wyrok Trybunału z dnia 22 czerwca 2022 r., *Leistritz AG przeciwko LH*, C-534/20, EU:C:2022:495, pkt 28.

26. Proponowane rozporządzenie zawiera zatem zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji, bez względu na to, czy są one wykorzystywane przez operatorów prywatnych czy przez organy publiczne, w tym, dodatkowo¹⁴, przez organy ścigania i organy sądowe.
27. Oprócz uregulowań odnoszących się do wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa, które podlega przepisom szczegółowym dotyczącym przetwarzania danych osobowych (zob. część III poniżej), proponowane rozporządzenie nie zawiera żadnych zharmonizowanych przepisów w zakresie wykorzystywania systemów sztucznej inteligencji wysokiego ryzyka. Jak wyjaśniono w pkt 18 i 19 powyżej, odniesienie do wykorzystywania systemów sztucznej inteligencji wysokiego ryzyka co do zasady dotyczy instrukcji obsługi produktu (art. 29) i jest powiązane z obowiązkami nałożonymi na twórców systemów. Jak podkreślono w pkt 22, decyzja o tym, czy organy ścigania lub organy sądowe mogą wykorzystywać system sztucznej inteligencji wysokiego ryzyka, który został zgodnie z prawem wprowadzony do obrotu na podstawie proponowanego rozporządzenia, podejmowana jest przez organy krajowe zgodnie z prawem krajowym.
28. W związku z tym art. 87 ust. 2 TFUE, a w szczególności jego lit. a), nie jest adekwatną podstawą prawną proponowanego rozporządzenia. Przepisy wniosku ani nie propagują, ani nie utrudniają gromadzenia, przechowywania, przetwarzania, analizowania i wymiany istotnych informacji. W przypadku gdy takie działania będą wykonywane przez organy ścigania, niezbędne będzie tylko przestrzeganie szeregu ogólnych, zharmonizowanych warunków w celu ochrony praw użytkowników. Podobnie, deklarowane cele proponowanego rozporządzenia nie obejmują opracowywania wspólnych technik dochodzeniowo-śledczych. Proponowane wymogi dotyczące wykorzystywania systemów sztucznej inteligencji wysokiego ryzyka nie ograniczają się jedynie do obszaru WSiSW i nie dotyczą współpracy policyjnej *sensu stricto* zdefiniowanej w TFUE.

¹⁴ Zob. opinia Trybunału, *Konwencja stambulska*, A-1/19, EU:C:2021:198, w szczególności pkt 298 i 301.

29. Jeśli chodzi o przepisy art. 5 ust. 4 proponowanego rozporządzenia, państwa członkowskie będą nadal uprawnione do podejmowania decyzji o zezwoleniu na wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa. Jeśli dane państwo członkowskie podejmie taką decyzję, ma obowiązek określić niezbędne szczegółowe przepisy dotyczące wniosku o uprzednie zezwolenie, wydania i wykonania takiego zezwolenia, jak również przepisy dotyczące powiązanych przestępstw, w przypadku których zezwoliło na wykorzystywanie danego systemu do celów prowadzenia postępowań przygotowawczych lub wnoszenia oskarżeń¹⁵. Z dyskusji przeprowadzonych na forum Rady wynika, że proponowane przepisy nie skutkowałyby przyznaniem nowych uprawnień odpowiednim organom krajowym. Przeciwnie – stosowanie istniejących lub ewentualnych przyszłych mechanizmów zostało doprecyzowane w celu zapewnienia ochrony prawa do prywatności i danych osobowych.
30. W związku z powyższym art. 114 TFUE jest jedyną adekwatną podstawą prawną zharmonizowanych przepisów dotyczących systemów sztucznej inteligencji wysokiego ryzyka, w tym systemów wykorzystywanych przez organy ścigania i organy sądowe, i żadna podstawa prawna z obszaru WSiSW zawarta w tytule V części trzeciej TFUE – taka jak art. 87 TFUE w odniesieniu do tych zharmonizowanych przepisów – nie jest uzasadniona ani adekwatna.

¹⁵ Warto zauważyć, że art. 5 ust. 4 wniosku jest pod pewnymi względami podobny do art. 15 ust. 1 dyrektywy 2002/58 o e-prywatności. W szczególności przewidziano w nim możliwość odstępiania przez państwa członkowskie od niektórych zakazów ustanowionych w prawie Unii. W świetle utrwalonego orzecznictwa przepisy krajowe mające stanowić odstępstwo od tego zakazu będą musiały być objęte zakresem stosowania prawa Unii, co z kolei spowoduje, że zastosowanie będzie mieć do nich Karta.

III. ADEKWATNOŚĆ ART. 16 TFUE JAKO DODATKOWEJ PODSTAWY PRAWNEJ

31. W proponowanym rozporządzeniu przewidziano art. 16 TFUE jako podstawę prawną przetwarzania danych osobowych w obszarze egzekwowania prawa, a w motywach 25 i 26 zamieszczono odniesienie do art. 6a protokołu nr 21 i art. 2a protokołu nr 22 w kontekście przetwarzania danych osobowych w obszarze zapobiegania przestępczości. Zdaniem Komisji art. 16 TFUE ma służyć wyłącznie jako podstawa prawna przepisów nakładających ograniczenia na przetwarzanie biometrycznych danych osobowych w sposób uzupełniający w porównaniu do dyrektywy 2016/680 („dyrektywa o ochronie danych w sprawach karnych”). Art. 5 ust. 1 lit. d) został co do zasady sformułowany jako zakaz, od którego istnieją trzy wyjątki. Konkretnie rzecz ujmując, zakazuje się wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa, chyba że jest to absolutnie niezbędne do: (a) ukierunkowanego poszukiwania potencjalnych ofiar przestępstw, (b) zapobieżenia bezpośredniemu atakowi terrorystycznemu lub atakowi na integralność cielesną / życie osób fizycznych, (c) zlokalizowania lub zidentyfikowania lub ścigania sprawcy poważnego przestępstwa lub osoby podejrzanej o popełnienie takiego przestępstwa (z odniesieniem do europejskiego nakazu aresztowania). Kolejne wymogi określone w art. 5 ust. 2, 3 i 4 wiążą się z tym szczególnym wykorzystywaniem systemów sztucznej inteligencji przez organy ścigania, zwłaszcza z koniecznością przeprowadzenia oceny niezbędności i proporcjonalności, udzielenia uprzedniego zezwolenia (z wyjątkiem sytuacji nadzwyczajnych) i podjęcia przez państwa członkowskie decyzji o tym, czy zezwolić na krajowe konkretne wykorzystanie narzędzi sztucznej inteligencji w takich sytuacjach.
32. Art. 5 jest szczegółowym przepisem regulującym konkretne wykorzystywanie narzędzi sztucznej inteligencji, który nie tylko ma uzupełnić istniejące unijne ramy prawne (dyrektywę o ochronie danych w sprawach karnych, której podstawą jest również art. 16 TFUE), ale także zobowiązuje do ustanowienia krajowych ram wdrażania.

33. Co do zasady, pomimo tego, że przepis szczegółowy zawarty w art. 5 został sformułowany w formie zakazu, można uznać, że określa on ściśle i wyjątkowe ramy ogólnego monitorowania – za pomocą instrumentów sztucznej inteligencji – „w czasie rzeczywistym” osób znajdujących się w otwartej przestrzeni do celów ich identyfikacji. Zakaz wykracza także poza zwykłe stosowanie kamer do celów rejestrowania i odnosi się do wykorzystywania narzędzi sztucznej inteligencji do automatycznego rozpoznawania cech ludzkich w przestrzeni publicznej (takich jak twarz, ale również sposób chodzenia, odciski palców, DNA, głos, dynamika uderzania w klawisze i inne sygnały biometryczne lub behawioralne). Oznacza to również jednoczesne pobieranie danych i identyfikację osób poprzez porównanie / weryfikację danych w drodze analizy. Ponadto przepis ten należy także ocenić w świetle tego, że dozwolona może też być identyfikacja „w czasie rzeczywistym” w przestrzeni publicznej przez użytkowników prywatnych (w przypadku takich wydarzeń jak mecze piłki nożnej).
34. Z dalszych wyjaśnień przedstawionych przez Komisję wydaje się wynikać, że aktualnie żadne państwo członkowskie nie uregulowało tej konkretnej kwestii – lub że zrobiło to tylko kilka z nich – w celu umożliwienia organom ścigania stosowania narzędzi sztucznej inteligencji do wykrywania osób w przestrzeni publicznej „w czasie rzeczywistym”. W praktyce jednak – chociaż nie przedstawiono żadnych niepodważalnych dowodów na to, że trzeba będzie zmienić istniejące praktyki i narzędzia – wydaje się jasne, że przyszłe techniki dochodzeniowo-śledcze, metody kryminalistyczne i przepisy dotyczące przeprowadzania dowodów będą musiały uwzględniać to podejście oparte na zakazie / wyjątkach.
35. Jeżeli chodzi o podstawę prawną, wydaje się, że przepisy wprowadzające ograniczenia w przetwarzaniu biometrycznych danych osobowych w sposób uzupełniający (w porównaniu do dyrektywy o ochronie danych w sprawach karnych) mają na celu ochronę danych osobowych poprzez ustanowienie odpowiednich zabezpieczeń. Taki cel jest nierozdzielnie związany z celem przepisów opartych na art. 114 TUE, przy czym żaden z tych celów nie jest drugorzędny ani pośredni w stosunku do drugiego. Celem proponowanego rozporządzenia jest ustanowienie ogólnych ram dotyczących systemów sztucznej inteligencji zgodnie z podejściem opartym na analizie ryzyka. W tym kontekście horyzontalne uregulowanie systemów sztucznej inteligencji może obejmować ściśle zabezpieczenia mające zastosowanie do tego konkretnego systemu sztucznej inteligencji służącego do wykrywania osób „w czasie rzeczywistym”. Taki konkretny system sztucznej inteligencji zawierający odpowiednie zabezpieczenia w zakresie ochrony danych osobowych jest zatem nierozdzielnie związany z ogólnym celem poprawy funkcjonowania rynku wewnętrznego i nie jest drugorzędny ani pośredni w stosunku do tego celu. Proponowane rozporządzenie powinno zatem opierać się na podwójnej podstawie prawnej zgodnie z odpowiednim orzecznictwem (zob. pkt 9 powyżej).

36. Pozostaje do rozstrzygnięcia kwestia tego, którą podstawę prawną należy zastosować do uregulowania przetwarzania danych osobowych do celów wykorzystywania systemów, o których mowa w art. 5 ust. 1 lit. c) – ust. 4 proponowanego rozporządzenia. W rzeczy samej art. 87 ust. 2 lit. a) TFUE stanowi podstawę prawną środków stosowanych przez organy ścigania w odniesieniu do zapobiegania przestępstwom, ich wykrywania i prowadzenia w ich sprawie postępowań przygotowawczych, jeśli chodzi o gromadzenie, przechowywanie, przetwarzanie, analizowanie i wymianę istotnych informacji.
37. Jak wyjaśnił rzecznik generalny w opinii dotyczącej umowy z Kanadą o danych PNR (A1/15), art. 16 TFUE, z jednej strony, oraz art. 87 ust. 2 lit. a) i art. 82 ust. 1 lit. d) TFUE, z drugiej strony, nie mogą pozostawać w stosunkach typu hierarchicznego *lex generalis – lex specialis*¹⁶. Art. 16 ust. 2 TFUE jest jedynym przepisem mającym zastosowanie do przepisów dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez organy ścigania w państwach członkowskich podczas wykonywania przez te organy działań w zakresie zapobiegania przestępczości. Sam fakt, że art. 5 zawiera odniesienie do wykazu poważnych przestępstw zamieszczonego w decyzji ramowej o europejskim nakazie aresztowania, nie zmienia tej oceny: odniesienie to nie oznacza, że ta decyzja ramowa ma zastosowanie jako taka¹⁷. Wymienienie poważnych przestępstw tylko technika legislacyjna, dzięki której nie ma potrzeby tworzenia odrębnego załącznika.
38. Nie zmienia to faktu, że przepis zawarty w art. 5 ustanowiono nie jako sposób dalszego określania warunków stosowania tych środków związanych z WSiSW, ale w celu zapewnienia, by w przyszłości każdy przypadek wykorzystywania identyfikacji biometrycznej „w czasie rzeczywistym” przez systemy sztucznej inteligencji uwzględniał w adekwatny sposób obawy związane z prawami podstawowymi, a zwłaszcza wymóg zapewnienia, by dane biometryczne były gromadzone i przetwarzane z poszanowaniem prawa do prywatności i do ochrony danych osobowych.

W tym względzie proponowane rozporządzenie nie ma na celu ustanowienia nowej, obowiązkowej procedury w obszarze WSiSW, ale raczej opiera się na wypróbowanych i sprawdzonych środkach proceduralnych, które zapewniają poszanowanie praw podstawowych.

¹⁶ Zob. opinia rzecznika generalnego P. Mengozziego z dnia 8 września 2016 r., *Projekt umowy między Kanadą a Unią Europejską*, opinia w sprawie 1/15, EU:C:2016:656, pkt 112–120.

¹⁷ W odniesieniu do wdrażania tego wykazu poważnych przestępstw przez państwa członkowskie, zob. wyrok Trybunału z dnia 21 czerwca 2022 r., *Ligue des droits humains ASBL przeciwko Conseil des ministres*, C- 817/19, EU:C:2022:65, pkt 150–152.

39. Jeżeli art. 16 TFUE jest adekwatną podstawą prawną, powstaje pytanie co do stosowania odpowiednio art. 6a i 2a protokołów nr 21 i 22. Jak wyjaśniono w motywach 25 i 26 wniosku, oznacza to, że jeżeli organy ścigania w Irlandii lub w Danii wykorzystują systemy zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów zapobiegania przestępczości i jeżeli Irlandia lub Dania nie są związane odpowiednimi przepisami dotyczącymi współpracy policyjnej lub współpracy wymiarów sprawiedliwości w sprawach karnych, te dwa państwa członkowskie nie będą związane art. 5 ust. 1 lit. d), ust. 2 i 3 proponowanego rozporządzenia. Nie oznacza to, że art. 5 ust. 1 lit. d), ust. 2 i 3 zawierają przepisy dotyczące współpracy policyjnej, takie jak przepisy o wymianie informacji między organami ścigania. Oznacza to tylko tyle, że art. 5 ust. 1 lit. d), ust. 2 i 3 proponowanego rozporządzenia – podobnie jak dyrektywa 2016/680 (dyrektywa o ochronie danych w sprawach karnych), która jest *lex generalis* przyjętym na podstawie art. 16 TFUE – regulują przetwarzanie biometrycznych danych osobowych w szczególnym kontekście systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów zapobiegania przestępczości. W tym względzie wniosek Komisji jest zgodny z podejściem przyjętym przez unijnego prawodawcę w odniesieniu do dyrektywy o ochronie danych w sprawach karnych i tym samym potwierdza, że odniesienie do art. 87 ust. 2 TFUE w tym kontekście nie jest zatem uzasadnione.
40. Dodanie art. 16 TFUE do art. 114 TFUE w tym przypadku jest uzasadnione tym, że art. 5 ust. 1 lit. d), ust. 2 i 3 są jedynymi przepisami regulującymi wykorzystywanie systemu sztucznej inteligencji, na którego stosowanie zezwolono, a który ingeruje w prawo do ochrony danych osobowych, co stanowi *lex specialis* w stosunku do ogólnych ram ochrony danych. Takich przepisów *lex specialis* regulujących ochronę danych i mających wpływ na stosowanie tych wrażliwych systemów sztucznej inteligencji nie można uznać za wtórne ani pośrednie w odniesieniu do podstawy prawnej dotyczącej rynku wewnętrznego. Dodanie art. 16 TFUE jako podstawy prawnej jest zatem wystarczająco uzasadnione w proponowanym rozporządzeniu, a odniesienie do art. 87 ust. 2 lit. a) TFUE nie jest adekwatne.

IV. WNIOSEK

41. W związku z powyższym Służba Prawna uważa, że:

- a) odniesienie do art. 16 i 114 TFUE jako podstaw prawnych proponowanego rozporządzenia jest uzasadnione i adekwatne;
 - b) odniesienie do art. 87 ust. 2 TFUE lub jakiejkolwiek innej podstawy prawnej w obszarze WSiSW nie jest uzasadnione ani adekwatne w przypadku zharmonizowanych przepisów mających zastosowanie do systemów sztucznej inteligencji, które mogą być udostępniane lub wykorzystywane przez organy ścigania lub organy sądowe.
-