Parlament Europejski
2019-2024

Dokument z posiedzenia

A9-0232/2021

13.7.2021

SPRAWOZDANIE

w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych
(2020/2016(INI))

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

Sprawozdawca: Petar Vitanov

PR_INI

SPIS TREŚCI

Strona

PROJEKT REZOLUCJI PARLAMENTU EUROPEJSKIEGO

w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych
(2020/2016(INI))

Parlament Europejski,

– uwzględniając Traktat o Unii Europejskiej (TUE), w szczególności jego art. 2 i 6, oraz Traktat o funkcjonowaniu Unii Europejskiej (TFUE), w szczególności jego art. 16,

– uwzględniając Kartę praw podstawowych Unii Europejskiej (zwaną dalej Kartą), w szczególności jej art. 6, 7, 8, 11, 12, 13, 20, 21, 24 i 47,

– uwzględniając Konwencję o ochronie praw człowieka i podstawowych wolności,

– uwzględniając Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS 108) oraz zmieniający ją protokół (zwaną dalej konwencją 108+),

– uwzględniając europejską kartę etyczną dotyczącą stosowania sztucznej inteligencji w systemach sądownictwa karnego i środowiskach pokrewnych opracowaną przez Europejską Komisję na rzecz Efektywności Wymiaru Sprawiedliwości (CEPEJ) Rady Europy,

– uwzględniając komunikat Komisji z dnia 8 kwietnia 2019 r. zatytułowany „Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka” (COM(2019)0168),

– uwzględniając wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji (AI) opublikowane przez grupę ekspertów wysokiego szczebla Komisji ds. AI w dniu 8 kwietnia 2019 r.,

– uwzględniając białą księgę Komisji z dnia 19 lutego 2020 r. w sprawie sztucznej inteligencji – „Europejskie podejście do doskonałości i zaufania” (COM(2020)0065),

– uwzględniając komunikat Komisji z dnia 19 lutego 2020 r. zatytułowany „Europejska strategia w zakresie danych” (COM(2020)0066),

– uwzględniając 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)[1],

– uwzględniając dyrektywę 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

[1] Dz.U. L 119 z 4.5.2016, s. 1.

zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW[2],

– uwzględniając 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[3],

– uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[4],

– uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW[5],

– uwzględniając rezolucję z 19 czerwca 2020 r. w sprawie protestów antyrasistowskich po śmierci George'a Floyda[6],

– uwzględniając swoją rezolucję z dnia 14 marca 2017 r. w sprawie wpływu technologii dużych zbiorów danych na prawa podstawowe: prywatność, ochrona danych, niedyskryminacja, bezpieczeństwo i ściganie przestępstw[7],

– uwzględniając wysłuchanie w Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) w dniu 20 lutego 2020 r. na temat sztucznej inteligencji w prawie karnym oraz jej wykorzystania przez policję i organy wymiaru sprawiedliwości w sprawach karnych,

– uwzględniając sprawozdanie z wizyty komisji LIBE w Stanach Zjednoczonych w lutym 2020 r.,

– uwzględniając art. 54 Regulaminu,

– uwzględniając opinie przedstawione przez Komisję Rynku Wewnętrznego i Ochrony Konsumentów oraz Komisję Prawną,

– uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (A9-0232/2021),

A. mając na uwadze niezwykle obiecujący, a zarazem związany z zagrożeniami charakter ogólnie technologii cyfrowych, a w szczególności upowszechnienia przetwarzania i

[2] Dz.U. L 119 z 4.5.2016, s. 89.
[3] Dz.U. L 295 z 21.11.2018, s. 39.
[4] Dz.U. L 201 z 31.7.2002, s. 37.
[5] Dz.U. L 135 z 24.5.2016, s. 53.
[6] Teksty przyjęte, P9_TA(2020)0173.
[7] Dz.U. C 263 z 25.7.2018, s. 82.

analizy danych przez sztuczną inteligencję; mając na uwadze, że w ostatnich latach dokonano dużego skoku naprzód w rozwoju sztucznej inteligencji, czyniąc ją jedną ze strategicznych technologii XXI wieku, która może w znaczący sposób korzystnie wpływać na wydajność, dokładność i wygodę, a co za tym idzie przekłada się na pozytywne przemiany w gospodarce europejskiej i społeczeństwie, przy czym stwarza również poważne zagrożenia dla praw podstawowych i systemów demokratycznych opartych na praworządności; mając na uwadze, że sztuczna inteligencja nie powinna być postrzegana jako cel sam w sobie, lecz jako służące człowiekowi narzędzie, którego ostatecznym celem jest działanie dla dobra człowieka oraz zwiększenie potencjału i bezpieczeństwa ludzi;

B. mając na uwadze, że pomimo ciągłych postępów w zakresie szybkości przetwarzania komputerowego i pojemności pamięci, nie istnieją jak dotąd programy, które mogłyby dorównać ludzkiej elastyczności wobec szerszych zagadnień lub w zadaniach wymagających zrozumienia kontekstu lub krytycznej analizy; mając na uwadze, że niektóre rozwiązania oparte na sztucznej inteligencji osiągnęły poziom wydajności równy ludzkim ekspertom i specjalistom w wykonywaniu niektórych konkretnych zadań (np. technologie informatyczne w usługach prawniczych) i mogą dostarczać wyników w znacznie szybszym tempie i na szerszą skalę;

C. mając na uwadze, że niektóre państwa, w tym kilka państw członkowskich, w większym stopniu niż inne korzystają z rozwiązań opartych na sztucznej inteligencji lub z systemów wbudowanych wykorzystujących sztuczną inteligencję, w ściganiu przestępstw i wymiarze sprawiedliwości, co częściowo wynika z braku regulacji oraz z różnic regulacyjnych, które umożliwiają wykorzystywanie sztucznej inteligencji do określonych celów lub tego zabraniają; mając na uwadze, że coraz częstsze stosowanie sztucznej inteligencji w dziedzinie prawa karnego opiera się w szczególności na obietnicach, że ograniczy ona niektóre rodzaje przestępstw i doprowadzi do podejmowania bardziej obiektywnych decyzji; mając jednak na uwadze, że obietnice te nie zawsze okazują się prawdziwe;

D. mając na uwadze, że podstawowe prawa i wolności zapisane w Karcie powinny być zagwarantowane przez cały cykl życia sztucznej inteligencji i powiązanych z nią technologii, w szczególności w trakcie ich projektowania, opracowywania, wdrażania i stosowania, oraz że powinny one mieć zastosowanie do ścigania przestępstw we wszystkich okolicznościach;

E. mając na uwadze, że technologia sztucznej inteligencji powinna być rozwijana w taki sposób, aby stawiała ludzi w centrum uwagi, cieszyła się zaufaniem publicznym i zawsze służyła ludziom; mając na uwadze, że systemy oparte na sztucznej inteligencji powinny mieć ostateczną gwarancję, tj. być projektowane w taki sposób, aby zawsze mógł je wyłączyć operator będący człowiekiem;

F. mając na uwadze, że aby systemy oparte na sztucznej inteligencji były godne zaufania, jak opisano to w wytycznych w zakresie etyki opracowanych przez grupę ekspertów wysokiego szczebla ds. AI, muszą być rozliczalne, zaprojektowane z myślą o ochronie wszystkich i przynoszeniu korzyści wszystkim (w tym być projektowane z uwzględnieniem grup szczególnie narażonych na zagrożenia i zmarginalizowanych), nie mieć dyskryminacyjnego charakteru, być bezpieczne, podejmować wytłumaczalne i

przejrzyste decyzje, a także szanować autonomię człowieka i jego prawa podstawowe;

G. mając na uwadze, że na Unii i jej państwach członkowskich spoczywa zasadnicza odpowiedzialność w zakresie dopilnowania, by decyzje związane z cyklem życia i stosowaniem rozwiązań opartych na sztucznej inteligencji w obszarze wymiaru sprawiedliwości i ścigania przestępstw były podejmowane w sposób przejrzysty, gwarantowały poszanowanie praw podstawowych, a w szczególności nie utrwalały dyskryminacji, stronniczości lub uprzedzeń tam, gdzie takie istnieją; mając na uwadze, że odpowiednie wybory polityczne powinny być zgodne z zasadami konieczności i proporcjonalności, aby zagwarantować konstytucyjność oraz sprawiedliwy i ludzki system wymiaru sprawiedliwości;

H. mając na uwadze, że rozwiązania oparte na sztucznej inteligencji mogą oferować duże możliwości w dziedzinie ścigania przestępstw, w szczególności w zakresie usprawniania metod pracy organów ścigania i organów wymiaru sprawiedliwości oraz skuteczniejszego zwalczania niektórych rodzajów przestępstw, w szczególności przestępstw finansowych, prania pieniędzy i finansowania terroryzmu, niegodziwego traktowania dzieci w celach seksualnych i seksualnego wykorzystywania dzieci w internecie oraz niektórych rodzajów cyberprzestępstw, przyczyniając się w ten sposób do zwiększenia bezpieczeństwa i ochrony obywateli UE, a jednocześnie mogąc się wiązać ze znacznymi zagrożeniami dla praw podstawowych ludzi; mając na uwadze, że powszechne stosowanie sztucznej inteligencji do celów masowej inwigilacji byłoby nieproporcjonalne;

I. mając na uwadze, że opracowywanie i obsługa systemów opartych na sztucznej inteligencji dla potrzeb policji i organów wymiaru sprawiedliwości wiąże się z udziałem wielu osób i organizacji, z wykorzystaniem licznych podzespołów urządzeń i algorytmów oprogramowania oraz z uczestnictwem wielu użytkowników ludzkich w często złożonych i wymagających warunkach; mając na uwadze, że stosowane w ściganiu przestępstw i wymiarze sprawiedliwości rozwiązania oparte na sztucznej inteligencji znajdują się na różnych etapach rozwoju, począwszy od opracowywania koncepcji, przez tworzenie prototypów, ocenę, a skończywszy na użytkowaniu zatwierdzonych już rozwiązań; mając na uwadze, że trwające na całym świecie badania naukowe mogą prowadzić do nowych zastosowań w przyszłości w miarę doskonalenia się technologii;

J. mając na uwadze, że konieczne jest ustanowienie jasnego modelu odpowiedzialności prawnej za potencjalnie szkodliwe skutki systemów sztucznej inteligencji w obszarze wymiaru sprawiedliwości w sprawach karnych; mając na uwadze, że prawodawstwo w tej dziedzinie powinno zawsze zachować odpowiedzialność człowieka i mieć na celu przede wszystkim uniknięcie szkodliwych skutków;

K. mając na uwadze, że w przypadku wykorzystywania systemów sztucznej inteligencji w dziedzinie ścigania przestępstw i wymiaru sprawiedliwości odpowiedzialność za zagwarantowanie pełnego poszanowania praw podstawowych spoczywa ostatecznie na państwach członkowskich;

L. mając na uwadze, że związek między ochroną praw podstawowych a skutecznymi działaniami policyjnymi musi zawsze stanowić zasadniczy element dyskusji na temat

ewentualności i sposobu wykorzystywania sztucznej inteligencji w ściganiu przestępstw, w ramach którego decyzje mogą mieć długotrwałe konsekwencje dla życia i wolności poszczególnych osób; mając na uwadze, że jest to szczególnie ważne, ponieważ sztuczna inteligencja może stać się stałym elementem naszego ekosystemu sądownictwa karnego poprzez dostarczanie analiz i pomocy w czynnościach dochodzeniowych;

M. mając na uwadze, że organy ścigania korzystają z rozwiązań sztucznej inteligencji obejmujących technologie rozpoznawania twarzy, np. do przeszukiwania podejrzanych baz danych i identyfikacji ofiar handlu ludźmi lub wykorzystywania i niegodziwego traktowania dzieci w celach seksualnych, zautomatyzowane rozpoznawanie tablic rejestracyjnych, identyfikacja głosu, identyfikacja sposobu mówienia, technologia czytania z ruchu warg, nasłuch (np. algorytmy wykrywające strzały), autonomiczne przeszukiwanie i analizowanie wykrytych baz danych, przewidywanie (prognozowanie przestępczości i obszarów szczególnie narażonych na przestępczość), narzędzia do wykrywania zachowań, zaawansowane narzędzia autopsji wirtualnej pomagające ustalić przyczynę zgonu, autonomiczne narzędzia wykrywania nadużyć finansowych i finansowania terroryzmu, monitorowanie mediów społecznościowych (wyszukiwanie informacji i gromadzenie danych w celu eksploracji powiązań) oraz zautomatyzowane systemy dozoru obejmujące różne możliwości wykrywania (takie jak wykrywanie pulsu i kamery termowizyjne); mając na uwadze, że powyższe rozwiązania wraz z innymi potencjalnymi lub przyszłymi rozwiązaniami opartymi na technologii sztucznej inteligencji w dziedzinie ścigania przestępstw mogą cechować się bardzo zróżnicowanym stopniem wiarygodności i dokładności oraz wpływu na prawa podstawowe i dynamikę systemów sądownictwa karnego; mając na uwadze, że wiele z tych narzędzi jest stosowanych w państwach niebędących członkami UE, jednak ich stosowanie w Unii byłoby zgodnie z unijnym dorobkiem prawnym i orzecznictwem w dziedzinie ochrony danych nielegalne; mając na uwadze, że rutynowe wdrażanie algorytmów, nawet przy niewielkim odsetku wyników fałszywie dodatnich, może skutkować fałszywymi alarmami, których liczba będzie znacznie przewyższać liczbę prawidłowych alarmów;

N. mając na uwadze, że narzędzia i aplikacje oparte na sztucznej inteligencji są również wykorzystywane przez organy wymiaru sprawiedliwości kilku krajów na całym świecie, w tym do uzasadniania decyzji w sprawie tymczasowego aresztowania, wydawania wyroków, obliczania prawdopodobieństwa ponownego popełnienia przestępstwa i określania warunków zwolnienia warunkowego, internetowego rozstrzygania sporów, zarządzania orzecznictwem i zapewniania ułatwionego dostępu do pomocy prawnej; mając na uwadze, że doprowadziło to do wypaczenia i zmniejszenia szans osób o kolorze skóry innym niż biały i innych mniejszości; mając na uwadze, że ich stosowanie w UE, poza kilkoma państwami członkowskimi, jest obecnie w dużej mierze ograniczone do dziedziny prawa cywilnego;

O. mając na uwadze, że korzystanie ze sztucznej inteligencji przez organy ścigania wiąże się z szeregiem potencjalnie dużych i, w niektórych przypadkach, niedopuszczalnych zagrożeń naruszenia praw podstawowych jednostki, takich jak nieprzejrzyste podejmowanie decyzji, różne formy dyskryminacji i błędy występujące w podstawowym algorytmie, które mogą zostać wzmocnione przez przekazywanie informacji zwrotnej, a także ryzyko naruszenia prywatności i ochrony danych

osobowych, ryzyko ograniczenia swobody wypowiedzi i dostępu do informacji, zagrożenie dla domniemania niewinności, dostępu do skutecznego środka prawnego, prawa do rzetelnego procesu sądowego, a także dla wolności i bezpieczeństwa osób;

P. mając na uwadze, że systemy sztucznej inteligencji wykorzystywane przez organy ścigania i wymiar sprawiedliwości, są także podatne na ataki oparte na sztucznej inteligencji lub na „zatrucie" danych polegające na celowym wykorzystaniu niewłaściwego zestawu danych w celu uzyskania nieobiektywnych wyników; mając na uwadze, że w takich sytuacjach powstałe szkody mogą być jeszcze większe i mogą powodować gwałtownie większe szkody zarówno dla pojedynczych osób, jak i grup;

Q. mając na uwadze, że wdrożenie sztucznej inteligencji w organach ścigania i w wymiarze sprawiedliwości nie powinno być postrzegane jako zwykła opcja techniczna, lecz raczej jako decyzja polityczna w sprawie kształtu i celów systemów ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych; mając na uwadze, że nowoczesne prawo karne opiera się na założeniu, że władze reagują na przestępstwo po jego popełnieniu, bez zakładania, że wszyscy ludzie są niebezpieczni i w związku z tym muszą być stale monitorowani w celu zapobiegania potencjalnym naruszeniom; mając na uwadze, że techniki inwigilacji oparte na sztucznej inteligencji mocno podważają to podejście i wymagają od organów regulacyjnych na całym świecie pilnej i gruntownej oceny konsekwencji zezwalania na wprowadzenie technologii, które ograniczają rolę człowieka w ściganiu przestępstw i orzekaniu;

1. ponownie podkreśla, że ze względu na to, że działanie sztucznej inteligencji opiera się o przetwarzanie dużych ilości danych osobowych, prawo ochrony życia prywatnego i prawo do ochrony danych osobowych ma zastosowanie do wszystkich obszarów wykorzystywania sztucznej inteligencji oraz że należy w pełni przestrzegać unijnych ram prawnych dotyczących ochrony danych i prywatności; przypomina w związku z tym, że UE ustanowiła już standardy ochrony danych w zakresie ścigania przestępstw, które będą stanowić podstawę wszelkich przyszłych przepisów dotyczących stosowania sztucznej inteligencji w obszarze ścigania przestępstw i wymiarze sprawiedliwości; przypomina, że przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne, cele przetwarzania powinny być określone, jednoznaczne i zgodne z prawem, przetwarzanie powinno być adekwatne, stosowne i nie powinno wykraczać poza cele przetwarzania, powinno być dokładne i aktualne, a niedokładne dane, o ile nie mają zastosowania ograniczenia, powinny być poprawiane lub usuwane, dane powinny być przechowywane nie dłużej niż jest to konieczne i że należy ustalić jasne i odpowiednie terminy usunięcia takich danych lub okresowego przeglądu potrzeby ich bezpiecznego przechowywania; podkreśla ponadto, że należy zapobiegać możliwości identyfikacji osób za pomocą aplikacji opartych na sztucznej inteligencji z wykorzystaniem wcześniej zanonimizowanych danych;

2. ponownie potwierdza, że wszystkie rozwiązania dla organów ścigania i wymiaru sprawiedliwości opierające się na sztucznej inteligencji muszą być również wykorzystywane w pełnym poszanowaniu godności człowieka, zasad niedyskryminacyjnego traktowania, swobody przemieszczania się, domniemania niewinności oraz prawa do obrony, w tym prawa do zachowania milczenia, wolności wypowiedzi i swobodnego dostępu do informacji, wolności zgromadzeń i swobody stowarzyszania się, równości wobec prawa, zasady równości stron oraz prawa do

skutecznego środka odwoławczego i sprawiedliwego procesu zgodnie z Kartą praw podstawowych i europejską konwencją praw człowieka; podkreśla, że należy zakazać stosowania sztucznej inteligencji, które jest niezgodne z prawami podstawowymi;

3. przyznaje, że tempo opracowywania rozwiązań opartych na sztucznej inteligencji na całym świecie nie pozwala na sporządzenie wyczerpującego wykazu zastosowań, co stwarza potrzebę jasnego i spójnego modelu zarządzania gwarantującego zarówno prawa podstawowe jednostki, jak i jasność prawa dla podmiotów opracowujących, biorąc pod uwagę ciągły rozwój technologiczny; uważa jednak, że z uwagi na zadania i zakres odpowiedzialności policji i organów wymiaru sprawiedliwości oraz wpływ podejmowanych przez nie decyzji w odniesieniu do działań zapobiegawczych, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych oraz wykonywania kar korzystanie z rozwiązań opartych na sztucznej inteligencji należy uznać za obarczone wysokim ryzykiem w przypadkach, w których istnieje możliwość znacznego wpływu na życie osób fizycznych;

4. uważa w związku z tym, że wszelkie narzędzia wykorzystujące sztuczną inteligencję opracowane dla organów ścigania lub wymiaru sprawiedliwości i przez nie użytkowane powinny być co najmniej bezpieczne, rzetelne, zabezpieczone i adekwatne do zakładanych celów, powinny być zgodne z zasadami sprawiedliwości, minimalizacji danych, rozliczalności, przejrzystości, niedyskryminacji i wyjaśnialności, zaś ich opracowywanie, wdrażanie i stosowanie powinno podlegać ocenie ryzyka i ścisłej weryfikacji ich konieczności i proporcjonalności, z zabezpieczeniami proporcjonalnymi do stwierdzonego ryzyka; podkreśla, że zaufanie obywateli do stosowania opracowywanej, wdrażanej i wykorzystywanej w UE sztucznej inteligencji jest uzależnione od pełnego spełnienia wymienionych kryteriów;

5. uznaje pozytywny wkład niektórych rodzajów zastosowań sztucznej inteligencji w pracę organów ścigania i organów wymiaru sprawiedliwości w całej Unii; zwraca uwagę na przykład na usprawnienie zarządzania zbiorami orzecznictwa osiągnięte dzięki narzędziom umożliwiającym korzystanie z dodatkowych opcji wyszukiwania; uważa, że sztuczna inteligencja ma szereg innych możliwych zastosowań w ściganiu przestępstw i wymiarze sprawiedliwości, które można by zbadać, biorąc pod uwagę pięć zasad karty etycznej dotyczącej stosowania sztucznej inteligencji w systemach sądownictwa karnego i środowiskach pokrewnych, przyjętej przez CEPEJ, zwracając szczególną uwagę na wskazane przez CEPEJ „zastosowania, które należy traktować z największą ostrożnością”;

6. podkreśla, że każdej technologii można nadać nowe zastosowanie i w związku z tym wzywa do ścisłej demokratycznej kontroli i niezależnego nadzoru nad wszystkimi technologiami opartymi na sztucznej inteligencji stosowanymi przez organy ścigania i organy wymiaru sprawiedliwości, zwłaszcza tymi, które mogą ewentualnie być wykorzystywane do masowej inwigilacji lub masowego profilowania; w związku z tym z wielkim zaniepokojeniem odnotowuje potencjał niektórych technologii sztucznej inteligencji wykorzystywanych do masowej inwigilacji w dziedzinie ścigania przestępstw; podkreśla prawny wymóg zapobiegania masowej inwigilacji z wykorzystaniem technologii sztucznej inteligencji, które z definicji nie są zgodne z zasadami konieczności i proporcjonalności, oraz zakazania stosowania rozwiązań, które mogą prowadzić do masowej inwigilacji;

7. podkreśla, że podejście przyjęte w niektórych państwach nienależących do UE w odniesieniu do opracowywania, wdrażania i stosowania technologii masowej inwigilacji w sposób nieproporcjonalny narusza prawa podstawowe i w związku z tym nie może być stosowane przez UE; podkreśla w związku z tym, że zabezpieczenia przed niewłaściwym wykorzystaniem technologii sztucznej inteligencji przez organy ścigania i organy wymiaru sprawiedliwości muszą być również uregulowane w jednolity sposób w całej Unii;

8. zwraca uwagę na potencjał w zakresie stronniczości i dyskryminacji związany z wykorzystywaniem rozwiązań opartych na sztucznej inteligencji, np. wynikający z uczenia się maszyn, w tym z algorytmów, na których opierają się takie rozwiązania; zauważa, że uprzedzenia mogą być nieodłączną cechą podstawowych zbiorów danych, szczególnie jeżeli używa się danych historycznych, wprowadzonych przez twórców algorytmów lub wygenerowanych na etapie wdrażania systemów w realnym kontekście; zwraca uwagę, że na wyniki osiągane przez rozwiązania oparte na sztucznej inteligencji siłą rzeczy wpływa jakość wykorzystywanych danych oraz że takie nieodłączne uprzedzenia mają tendencję do stopniowego zwiększania się, a tym samym do utrwalania i pogłębiania istniejącej dyskryminacji, zwłaszcza w odniesieniu do osób należących do niektórych grup etnicznych lub społeczności rasowych;

9. podkreśla fakt, że wiele obecnie stosowanych technologii identyfikacji opartych na algorytmach w sposób nieproporcjonalny błędnie identyfikuje i błędnie klasyfikuje osoby o odmiennej rasie, osoby należące do określonych społeczności etnicznych, osoby LGBTI, dzieci i osoby starsze, a także kobiety, a tym samym im szkodzi; przypomina, że osoby fizyczne mają nie tylko prawo do tego, aby ich tożsamość została prawidłowo ustalona, ale także prawo do tego, aby ich tożsamość nie była w ogóle ustalana, o ile nie wymagają tego przepisy prawa ze względu na istotny i uzasadniony interes publiczny; podkreśla, że prognozowanie sztucznej inteligencji oparte na cechach charakterystycznych określonej grupy osób wzmacniają i powielają istniejące formy dyskryminacji; uważa, że należy dołożyć wszelkich starań, aby uniknąć zautomatyzowanej dyskryminacji i uprzedzeń; wzywa do wprowadzenia solidnych dodatkowych zabezpieczeń w przypadkach, gdy systemy oparte na sztucznej inteligencji stosowane w organach ścigania lub wymiarze sprawiedliwości są wykorzystywane w odniesieniu do nieletnich lub w związku z nimi;

10. zwraca uwagę na asymetryczny układ sił pomiędzy podmiotami stosującymi technologie sztucznej inteligencji a podmiotami podlegającymi działaniu tych technologii; podkreśla, że nadrzędne znaczenie ma zadbanie o to, aby stosowanie narzędzi sztucznej inteligencji przez organy ścigania i organy wymiaru sprawiedliwości nie stało się czynnikiem prowadzącym do nierówności, podziałów społecznych lub wykluczenia; zwraca uwagę na wpływ stosowania narzędzi sztucznej inteligencji na prawo podejrzanych do obrony, na trudności w uzyskaniu istotnych informacji na temat funkcjonowania tych narzędzi oraz wynikające z tego trudności w kwestionowaniu dostarczanych przez nie wyników przed sądem, w szczególności przez osoby objęte dochodzeniem;

11. zwraca uwagę na ryzyko związane w szczególności z wyciekiem danych, naruszeniami bezpieczeństwa danych oraz nieuprawnionym dostępem do danych osobowych i innych informacji związanych na przykład z dochodzeniami karnymi lub postępowaniami

sądowymi przetwarzanymi przez systemy sztucznej inteligencji; podkreśla, że należy dogłębnie przeanalizować aspekty zabezpieczenia i bezpieczeństwa systemów sztucznej inteligencji wykorzystywanych przez organy ścigania i wymiar sprawiedliwości, tak by systemy te były wystarczająco solidne i odporne, co pozwoli zapobiec potencjalnie katastrofalnym konsekwencjom złośliwych ataków na te systemy; podkreśla znaczenie uwzględniania bezpieczeństwa na etapie projektowania, a także szczególnego nadzoru ze strony człowieka przed uruchomieniem niektórych kluczowych zastosowań i w związku z tym wzywa organy ścigania i organy wymiaru sprawiedliwości, aby w celu zapobieżenia rozrostowi funkcji korzystały wyłącznie z zastosowań sztucznej inteligencji, które są zgodne z zasadą ochrony prywatności i ochrony danych już na etapie projektowania;

12. podkreśla, że żaden system oparty na sztucznej inteligencji wykorzystywany przez organy ścigania i organy wymiaru sprawiedliwości nie powinien być w stanie naruszać integralności cielesnej człowieka ani przyznawać osobom praw ani nakładać na nie obowiązków prawnych;

13. dostrzega wyzwania związane z właściwym przypisaniem odpowiedzialności prawnej i odpowiedzialności procesowej za potencjalne szkody, biorąc pod uwagę złożoność procesu opracowywania i funkcjonowania systemów opartych na sztucznej inteligencji; uważa za konieczne stworzenie jasnego i sprawiedliwego systemu przypisywania odpowiedzialności prawnej i odpowiedzialności procesowej za potencjalnie negatywne konsekwencje spowodowane przez te zaawansowane technologie cyfrowe; podkreśla jednak, że głównym celem musi być przede wszystkim zapobieganie wystąpieniu takich konsekwencji; wzywa zatem do stosowania zasady ostrożności w odniesieniu do wszystkich form wykorzystywania sztucznej inteligencji w obszarze ściganiu przestępstw; podkreśla, że odpowiedzialność prawna i odpowiedzialność procesowa musi zawsze spoczywać na osobie fizycznej lub prawnej, która musi być zawsze zidentyfikowana w przypadku decyzji podejmowanych przy wsparciu sztucznej inteligencji; podkreśla w związku z tym potrzebę zapewnienia przejrzystości struktur korporacyjnych, w których systemy sztucznej inteligencji są tworzone i zarządzane;

14. uważa, że zarówno dla skuteczności wykonywania prawa do obrony, jak i dla przejrzystości krajowych systemów wymiaru sprawiedliwości w sprawach karnych niezbędne jest, aby konkretne, jasne i precyzyjne ramy prawne regulowały warunki, zasady i konsekwencje stosowania narzędzi opartych na sztucznej inteligencji w obszarze ścigania przestępstw i sądownictwa, a także prawa osób poddanych działaniu tych narzędzi, w tym skuteczne i łatwo dostępne procedury składania skarg i dochodzenia roszczeń, łącznie z dochodzeniem odszkodowania na drodze sądowej; podkreśla, że strony postępowania karnego mają prawo dostępu do procesu gromadzenia danych oraz do ocen przeprowadzonych lub uzyskanych z zastosowaniem sztucznej inteligencji; podkreśla, że niezbędne jest, by – podejmując decyzję w sprawie wniosku o ekstradycję (lub wydanie) do innego państwa członkowskiego lub państwa trzeciego – wykonujące nakaz organy sądowe, które biorą udział we współpracy sądowej, oceniły, czy wykorzystanie narzędzi opartych na sztucznej inteligencji w państwie wnioskującym może jawnie naruszać podstawowe prawo do rzetelnego procesu sądowego; wzywa Komisję do wydania wytycznych dotyczących sposobu przeprowadzania takiej oceny w kontekście współpracy sądowej w sprawach karnych; podkreśla, że zgodnie z obowiązującymi przepisami państwa członkowskie powinny

dopilnować, by osoby fizyczne były informowane o tym, że stosowana jest wobec nich przez organy ścigania lub sądownictwo sztuczna inteligencja;

15. zwraca uwagę, że jeśli ludzie będą polegać wyłącznie na danych, profilach i zaleceniach generowanych przez maszyny, nie będą w stanie dokonać niezależnej oceny; podkreśla potencjalnie poważne negatywne konsekwencje, zwłaszcza w obszarze ścigania przestępstw i wymiaru sprawiedliwości, możliwe w przypadku gdy ludzie nadmiernie ufają pozornie obiektywnemu i naukowemu charakterowi narzędzi opartych na sztucznej inteligencji, nie biorąc pod uwagę możliwości, że ich wyniki są nieprawidłowe, niepełne, nieadekwatne lub dyskryminujące; podkreśla, że należy unikać nadmiernego polegania na wynikach dostarczanych przez systemy oparte na sztucznej inteligencji oraz zwraca uwagę na to, że konieczne jest, by władze nabyły pewności siebie i wiedzy niezbędnej do zakwestionowania lub uchylenia zalecenia algorytmicznego; uważa, że istotne jest, by mieć realistyczne oczekiwania wobec takich rozwiązań technologicznych i nie obiecywać doskonałych rozwiązań w zakresie ścigania przestępstw ani wykrywania wszystkich popełnionych przestępstw;

16. podkreśla, że w kontekście wymiaru sprawiedliwości i ścigania przestępstw każdą decyzję o skutkach prawnych lub równoważnych musi zawsze podejmować człowiek, którego można pociągnąć do odpowiedzialności za podjęte decyzje; uważa, że osoby, w których przypadku zastosowano systemy oparte na sztucznej inteligencji muszą mieć możliwość korzystania ze środków zaskarżenia; przypomina, że na mocy prawa UE osobom przysługuje prawo do tego, by nie podlegać decyzji, która wywołuje wobec nich skutki prawne lub w podobny sposób istotnie na nie wpływa, a opiera się jedynie na zautomatyzowanym przetwarzaniu danych; podkreśla ponadto, że proces podejmowania decyzji nie może opierać się na danych osobowych szczególnych kategorii, chyba że istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionego interesu osób, których dane dotyczą; podkreśla, że prawo UE zakazuje profilowania, które prowadzi do dyskryminacji osób fizycznych ze względu na szczególne kategorie danych osobowych; zwraca uwagę na fakt, że decyzje w dziedzinie ścigania przestępstw są prawie zawsze decyzjami, które rodzą skutki prawne dla osoby, której dotyczą, ze względu na wykonawczy charakter organów ścigania i ich działań; zauważa, że wykorzystywanie sztucznej inteligencji może wywierać wpływ na decyzje podejmowane przez ludzi i na wszystkie etapy postępowania karnego; w związku z tym jest zdania, że organy korzystające z systemów sztucznej inteligencji muszą przestrzegać niezwykle wysokich standardów prawnych i zapewniać interwencję człowieka, zwłaszcza podczas analizy danych pochodzących z takich systemów; w związku z tym domaga się, by utrzymać niezawisły osąd sędziów i podejmowanie decyzji na podstawie analizy poszczególnych przypadków; wzywa do wprowadzenia zakazu stosowania sztucznej inteligencji i związanych z nią technologii do celów proponowania orzeczeń sądowych;

17. wzywa do zadbania o to, by działania algorytmu można było wyjaśnić i by były one przejrzyste, identyfikowalne i weryfikowalne, tak aby można było zagwarantować, że opracowywanie, wdrażanie i wykorzystanie systemów sztucznej inteligencji w wymiarze sprawiedliwości i przez organy ścigania będzie zgodne z prawami podstawowymi i będzie cieszyło się zaufaniem obywateli, jak również aby móc dopilnować, by wyniki generowane przez algorytmy sztucznej inteligencji można było przedstawić w sposób zrozumiały dla użytkowników i tych, którzy są poddawani

działaniu tych systemów oraz by przejrzyste były informacje dotyczące danych źródłowych, jak również to, w jaki sposób system dochodzi do pewnych wniosków; zwraca uwagę, że aby zapewnić przejrzystość techniczną, odporność i dokładność, organy ścigania i sądownictwa w Unii powinny móc nabywać jedynie takie narzędzia i systemy, których algorytmy i logika poddają się kontroli i są dostępne co najmniej dla policji i sądownictwa, a także dla niezależnych audytorów, tak aby można było poddawać je ocenie, audytowi i weryfikacji, a ponadto takie narzędzia i systemy nie mogą być zamknięte lub oznaczone jako zastrzeżone przez sprzedawców; zwraca ponadto uwagę, że dokumentacja powinna być sporządzona w klarownym i zrozumiałym języku i dotyczyć charakteru usługi, wykorzystywanych narzędzi, sposobu działania i warunków, w jakich można oczekiwać, że będą one funkcjonować oraz ryzyka, jakie mogą stwarzać; wzywa w związku z tym organy sądownictwa i ścigania do proaktywnego zapewnienia pełnej przejrzystości odnośnie do prywatnych przedsiębiorstw, które dostarczają im systemy sztucznej inteligencji stosowane do celów ścigania przestępstw oraz wymiaru sprawiedliwości; zaleca w związku z tym korzystanie w miarę możliwości z otwartego oprogramowania;

18. zachęca organy ścigania i organy sądowe do określenia i oceny obszarów, w których niektóre dostosowane do potrzeb rozwiązania w zakresie sztucznej inteligencji mogą być korzystne, oraz do wymiany najlepszych praktyk w zakresie wdrażania sztucznej inteligencji; wzywa do przyjęcia przez państwa członkowskie i agencje UE odpowiednich procedur udzielania zamówień publicznych dotyczących systemów opartych na sztucznej inteligencji, gdy są one wykorzystywane w kontekście ścigania przestępstw lub wymiaru sprawiedliwości, tak aby zapewnić ich zgodność z prawami podstawowymi i obowiązującymi przepisami, w tym do zapewnienia, by dokumentacja oprogramowania i algorytmów była dostępna dla właściwych organów i organów nadzorczych w celów przeglądu; wzywa w szczególności do wprowadzenia wiążących przepisów określających wymóg publicznego ujawniania partnerstw publiczno-prywatnych, umów i zakupów oraz celu, do jakiego zostały pozyskane; podkreśla konieczność zapewnienia tym organom niezbędnych środków finansowych, a także wyposażenia ich w niezbędną wiedzę ekspercką w celu zagwarantowania pełnej zgodności z wymogami etycznymi, prawnymi i technicznymi związanymi z wszelkim wdrażaniem sztucznej inteligencji;

19. wzywa do zadbania o identyfikowalność systemów sztucznej inteligencji i procesów decyzyjnych, które określają działanie, możliwości i ograniczenia tych systemów, a także rejestrują pochodzenie elementów odpowiedzialnych za decyzje, na przykład poprzez obowiązkową dokumentację; podkreśla znaczenie prowadzenia pełnej dokumentacji danych treningowych, ich kontekstu, celu, dokładności i skutków ubocznych, a także przetwarzania tych danych przez twórców i twórców algorytmów oraz ich zgodności z prawami podstawowymi; podkreśla, że zawsze musi istnieć możliwość sprowadzenia obliczeń systemu opartego na sztucznej inteligencji do formy zrozumiałej dla ludzi;

20. wzywa do przeprowadzania obowiązkowej analizy skutków wszelkich systemów sztucznej inteligencji przeznaczonych dla organów ścigania i wymiaru sprawiedliwości przed ich wdrożeniem lub rozpoczęciem ich stosowania, by ocenić wszelkie ewentualne zagrożenia związane z naruszeniem praw podstawowych; przypomina, że uprzednia ocena skutków dla ochrony danych jest obowiązkowa w przypadku każdego rodzaju

przetwarzania, zwłaszcza przetwarzania z wykorzystaniem nowych technologii, które to przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, oraz jest zdania, że z takim wysokim ryzykiem mamy do czynienia w przypadku większości technologii sztucznej inteligencji wykorzystywanych w dziedzinie ścigania przestępstw i w sądownictwie; podkreśla wiedzę ekspercką organów ochrony danych i agencji praw podstawowych w dziedzinie oceny tych systemów; podkreśla, że te oceny skutków dla przestrzegania praw podstawowych powinny być przeprowadzane w sposób jak najbardziej otwarty i przy czynnym udziale społeczeństwa obywatelskiego; domaga się, aby w ocenach skutków wyraźnie określono również zabezpieczenia niezbędne do przeciwdziałania stwierdzonym zagrożeniom oraz aby oceny te zostały w jak najszerszym zakresie udostępnione publicznie przed wdrożeniem jakiegokolwiek systemu sztucznej inteligencji;

21. podkreśla, że tylko dzięki rzetelnemu zarządzaniu europejską sztuczną inteligencją, a także niezależnej ocenie, możliwe będzie tak konieczne zastosowanie w praktyce zasad dotyczących praw podstawowych; wzywa do okresowego, obowiązkowego audytu wszystkich systemów sztucznej inteligencji wszędzie tam, gdzie mogą one w istotnym stopniu wpływać na życie jednostek, przy czym audyt ten ma prowadzić niezależny organ, mając na celu sprawdzenie i ocenę systemów algorytmicznych, ich kontekstu, celu, dokładności, wydajności i skali oraz – podczas działania systemów – aby wykryć, przeanalizować, zdiagnozować i usunąć wszelkie niepożądane i negatywne skutki tych systemów oraz zapewnić, by systemy sztucznej inteligencji działały zgodnie z przyjętymi założeniami; wzywa zatem do stworzenia w tym celu jasnych ram instytucjonalnych, w tym odpowiedniego nadzoru regulacyjnego i nadzorczego, w celu zapewnienia pełnego wdrożenia i zagwarantowania w pełni świadomej demokratycznej debaty na temat konieczności i proporcjonalności sztucznej inteligencji w dziedzinie wymiaru sprawiedliwości w sprawach karnych; podkreśla, że wyniki tych audytów powinny być udostępniane w rejestrach publicznych, tak aby obywatele wiedzieli, czy stosowane są systemy oparte na sztucznej inteligencji i jakie środki są podejmowane w celu zaradzenia wszelkim naruszeniom praw podstawowych;

22. podkreśla, że zbiory danych i systemy algorytmiczne stosowane przy klasyfikowaniu, ocenianiu i prognozowaniu na różnych etapach przetwarzania danych w ramach opracowywania sztucznej inteligencji i związanych z nią technologii mogą również prowadzić do odmiennego traktowania oraz zarówno bezpośredniej, jak i pośredniej dyskryminacji grup osób, zwłaszcza jeśli dane wykorzystywane do treningu algorytmów służących do prognozowania przestępczości odzwierciedlają bieżące priorytety w zakresie nadzoru i w związku z tym mogą prowadzić do powielania i wzmacniania istniejących form dyskryminacji; podkreśla, że technologie sztucznej inteligencji – zwłaszcza te opracowywane w celu wykorzystania w obszarze ścigania przestępstw i sądownictwa – wymagają interdyscyplinarnych badań i wkładu, w tym w dziedzinie studiów naukowych i technologicznych, studiów w dziedzinie krytycznej teorii rasy, studiów nad niepełnosprawnością oraz innych dyscyplin uwzględniających kontekst społeczny, w tym dotyczących sposobu konstruowania różnic, działania klasyfikacji i jej konsekwencji; podkreśla zatem konieczność systematycznego inwestowania w uwzględnianie tych dyscyplin w ramach studiów i badań nad sztuczną inteligencją prowadzonych na wszystkich szczeblach; podkreśla również, że ważne jest, by zespoły, które projektują, opracowują, testują, serwisują, wdrażają i zamawiają te systemy sztucznej inteligencji do celów ścigania przestępstw i sądownictwa

odzwierciedlały – w miarę możliwości – różnorodność społeczeństwa, co będzie służyć jako nietechniczny sposób na zmniejszenie ryzyka dyskryminacji;

23. podkreśla również, że odpowiednia rozliczalność, odpowiedzialność prawna i odpowiedzialność procesowa wymagają wielu specjalistycznych szkoleń z zakresu przepisów etycznych, potencjalnych zagrożeń, ograniczeń i właściwego korzystania z technologii sztucznej inteligencji, zwłaszcza dla pracowników organów policji i wymiaru sprawiedliwości; podkreśla, że osoby podejmujące decyzje powinny posiadać odpowiednie przeszkolenie zawodowe i kwalifikacje w kwestii potencjału stronniczości, ponieważ zbiory danych mogą zawierać dane oparte na dyskryminacji i uprzedzeniach; popiera ustanowienie inicjatyw uświadamiających i edukacyjnych mających zagwarantować, że osoby pracujące w organach ścigania i wymiarze sprawiedliwości są świadome ograniczeń, możliwości i zagrożeń, jakie wiążą się z wykorzystaniem systemów opartych na sztucznej inteligencji, w tym ryzyka uprzedzeń związanych z automatyzacją, oraz że te ograniczenia, możliwości i zagrożenia rozumieją; przypomina, że włączenie do treningowych zbiorów danych, które służą sztucznej inteligencji, przypadków rasizmu ze strony sił policyjnych przy wypełnianiu ich obowiązków nieuchronnie doprowadzi do rasistowskiej stronniczości w ustaleniach, wynikach i zaleceniach generowanych przez sztuczną inteligencję; w związku z tym ponownie wzywa państwa członkowskie do promowania polityki antydyskryminacyjnej oraz do opracowania krajowych planów działania przeciwko rasizmowi w odniesieniu do policji i systemu wymiaru sprawiedliwości,

24. zauważa, że prognozowanie przestępczości należy do rozwiązań opartych na sztucznej inteligencji stosowanych w obszarze ścigania przestępstw, ale ostrzega, że choć prognozowanie przestępczości może analizować dane zbiory danych w celu określenia schematów i korelacji, nie może odpowiedzieć na pytanie o przyczynowość i nie może wiarygodnie prognozować indywidualnych zachowań, a zatem nie może stanowić jedynej podstawy interwencji; zwraca uwagę, że kilka miast w Stanach Zjednoczonych – po przeprowadzeniu audytów – zaprzestało stosowania systemów prognozowania przestępczości; przypomina, że podczas wizyty komisji LIBE w Stanach Zjednoczonych w lutym 2020 r. posłowie zostali poinformowani przez wydziały policji Nowego Jorku i Cambridge (w stanie Massachusetts), że z powodu braku skuteczności, dyskryminującego wpływu i nieskuteczności w praktyce zrezygnowali ze swoich programów prognozowania przestępczości i zaczęli w zamian wdrażać koncepcję policji środowiskowej; zauważa, że doprowadziło to do spadku przestępczości; w związku z tym sprzeciwia się wykorzystywaniu przez organy ścigania sztucznej inteligencji do przewidywania zachowań jednostek lub grup na podstawie danych historycznych i wcześniejszych zachowań, a także na podstawie przynależności do grupy, lokalizacji lub wszelkich innych tego rodzaju cech w ramach prób wskazywania osób mogących popełnić przestępstwo;

25. zauważa, że istnieją różne rodzaje zastosowania rozpoznawania twarzy, takie jak między innymi weryfikacja/uwierzytelnianie (tj. porównywanie wizerunku twarzy obecnej osoby ze zdjęciem na dokumencie tożsamości, (np. w ramach inteligentnych granic), identyfikowanie (tj. dopasowywanie zdjęcia do danych z danej bazy zdjęć) oraz wykrywanie (tj. wyodrębnianie wizerunku twarzy w czasie rzeczywistym z wykorzystaniem takich źródeł jak materiały zarejestrowane przez system monitoringu wizyjnego i przeszukiwanie baz danych w celu dopasowania wizerunku (np. nadzór w

czasie rzeczywistym), a każde z tych zastosowań ma inne konsekwencje pod względem ochrony praw podstawowych; zdecydowanie uważa, że korzystanie z systemów rozpoznawania twarzy przez organy ścigania powinno być ograniczone do ściśle określonych celów przy pełnym poszanowaniu zasad proporcjonalności i konieczności oraz obowiązującego prawa; ponownie przypomina, że wykorzystanie technologii rozpoznawania twarzy musi co najmniej spełniać wymogi minimalizacji danych, dokładności danych, ograniczenia ich przechowywania, bezpieczeństwa danych i odpowiedzialności za nie, a także być zgodne z prawem, sprawiedliwe, przejrzyste i zgodne z konkretnym, wyraźnym i uzasadnionym celem, który jest jasno określony w prawie danego państwa członkowskiego lub Unii; jest zdania, że systemy weryfikacji i uwierzytelniania można nadal wdrażać i stosować z powodzeniem tylko wtedy, gdy ich negatywne skutki poddają się działaniom łagodzącym, oraz gdy spełnić można powyższe kryteria;

26. wzywa ponadto do wprowadzenia stałego zakazu stosowania automatycznej analizy lub automatycznego rozpoznawania w przestrzeni publicznej innych cech ludzkich, takich jak chód, odciski palców, DNA, głos i inne elementy biometryczne i behawioralne;

27. wzywa jednak do przyjęcia moratorium na korzystanie z systemów rozpoznawania twarzy do działań organów ścigania, które mają na celu identyfikację, chyba że rozpoznawanie twarzy służy wyłącznie identyfikacji ofiar przestępstw, dopóki nie będzie można uznać, że standardy techniczne są w pełni zgodne z prawami podstawowymi, uzyskane wyniki są bezstronne i nikogo nie dyskryminują, ramy prawne zapewniają solidne zabezpieczenia przed niewłaściwym wykorzystaniem oraz ścisłą kontrolę i nadzór demokratyczny, a konieczność i proporcjonalność wprowadzenia takich technologii została potwierdzona dowodami empirycznymi; zauważa, że jeżeli powyższe kryteria nie są spełnione, systemy nie powinny być wdrażane ani stosowane;

28. wyraża ogromne zaniepokojenie wykorzystywaniem przez organy ścigania i służby wywiadowcze prywatnych baz danych służących do rozpoznawania twarzy, takich jak baza danych Clearview AI zawierająca ponad trzy miliardy zdjęć, które zostały pozyskane nielegalnie z sieci społecznościowych i innych miejsc w internecie, w tym od obywateli UE; wzywa państwa członkowskie do nałożenia na organy ścigania obowiązku ujawniania, czy korzystają one z technologii Clearview AI lub równoważnych technologii pochodzących od innych dostawców; przypomina opinię Europejskiej Rady Ochrony Danych (EROD), zgodnie z którą korzystanie przez organy ścigania w Unii Europejskiej z usługi takiej jak Clearview AI „prawdopodobnie nie byłoby zgodne z unijnym systemem ochrony danych”; wzywa do wprowadzenia zakazu korzystania z prywatnych baz danych służących do rozpoznawania twarzy w ramach ścigania przestępstw;

29. przyjmuje do wiadomości sporządzone przez Komisję studium wykonalności dotyczące możliwych zmian w decyzji w sprawie konwencji z Prüm[8], w tym w kwestii wizerunków twarzy; przyjmuje do wiadomości wcześniejsze badania, z których wynika, że żadne ewentualne nowe identyfikatory, np. tęczówka lub rozpoznawanie twarzy, nie byłyby tak wiarygodne w kontekście kryminalistycznym jak DNA czy odciski palców;

[8] Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej; Dz.U. L 210 z 6.8.2008, s. 1.

przypomina Komisji, że każdy wniosek ustawodawczy musi opierać się na dowodach i być zgodny z zasadą proporcjonalności; wzywa Komisję do powstrzymania się od rozszerzenia ram decyzji z Prüm, chyba że będą istnieć solidne dowody naukowe potwierdzające wiarygodność rozpoznawania twarzy w kontekście kryminalistycznym w porównaniu z rozpoznawaniem w oparciu o DNA lub odciski palców, po wcześniejszym przeprowadzeniu przez nią pełnej oceny skutków oraz po uwzględnieniu zaleceń Europejskiego Inspektora Ochrony Danych (EIOD) i EROD;

30. podkreśla, że wykorzystanie danych biometrycznych wiąże się w szerszym ujęciu z zasadą prawa do godności ludzkiej, na której opierają się wszystkie prawa podstawowe gwarantowane przez Kartę; uważa, że wykorzystywanie i gromadzenie wszelkich danych biometrycznych do celów zdalnej identyfikacji, np. poprzez rozpoznawanie twarzy w miejscach publicznych, a także przy automatycznych bramkach kontroli granicznej wykorzystywanych do odprawy granicznej na lotniskach, może stanowić szczególne zagrożenie dla praw podstawowych, przy czym skutki mogą się znacznie różnić w zależności od celu, kontekstu i zakresu stosowania; następnie podkreśla, że technologie rozpoznawania emocji, takie jak kamery wykrywające ruchy oczu i zmiany wielkości źrenic mają kwestionowalną wiarygodność naukową w kontekście ściganie przestępstw; jest zdania, że stosowanie identyfikacji biometrycznej w kontekście ścigania przestępstw i sądownictwa powinno zawsze być uznawane za „wysokie ryzyko” i w związku z tym podlegać dodatkowym wymogom, zgodnie z zaleceniami powołanej przez Komisję grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji;

31. wyraża głębokie zaniepokojenie projektami badawczymi finansowanymi w ramach programu „Horyzont 2020”, w których wykorzystuje się sztuczną inteligencję na granicach zewnętrznych, takimi jak projekt iBorderCtrl, który jest testowanym na Węgrzech, Łotwie i w Grecji „inteligentnym systemem wykrywania kłamstw” profilującym podróżnych na podstawie zautomatyzowanego komputerowo wywiadu przeprowadzonego za pomocą kamery internetowej podróżnego przed podróżą oraz na podstawie opartej na sztucznej inteligencji analizy 38 mikrogestów; wzywa w związku z tym Komisję do wprowadzenia, za pomocą środków ustawodawczych i nieustawodawczych, a w razie potrzeby w drodze postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego, zakazu prowadzenia do celów ścigania przestępstw jakiegokolwiek przetwarzania danych biometrycznych, które skutkuje masową inwigilacją w przestrzeni publicznej; wzywa ponadto Komisję do zaprzestania finansowania badań dotyczących systemów biometrycznych lub ich wdrażania, a także programów, które mogłyby doprowadzić do ogólnego masowego nadzoru w przestrzeni publicznej; podkreśla w tym kontekście, że należy zwrócić szczególną uwagę na wykorzystywanie dronów w operacjach policyjnych oraz wdrożyć rygorystyczne ramy ich stosowania;

32. popiera zalecenia powołanej przez Komisję grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji nawołujące do zakazu masowej klasyfikacji punktowej obywateli przy użyciu sztucznej inteligencji; uważa, że wszelkie formy normatywnej klasyfikacji punktowej obywateli prowadzonej na dużą skalę przez organy publiczne, zwłaszcza w dziedzinie ścigania przestępstw i wymiaru sprawiedliwości, prowadzą do utraty autonomii, zagrażają zasadzie niedyskryminacji i nie mogą być uznawane za zgodne z zapisanymi w ustawodawstwie UE prawami podstawowymi, zwłaszcza z godnością

ludzką;

33. wzywa do zwiększenia ogólnej przejrzystości, aby wypracować wszechstronne zrozumienie kwestii dotyczących stosowania sztucznej inteligencji w Unii; zwraca się do państw członkowskich o przekazanie wyczerpujących informacji o narzędziach wykorzystywanych przez ich organy ścigania i wymiaru sprawiedliwości z uwzględnieniem rodzajów wykorzystywanych narzędzi, celów, dla których są one wykorzystywane, rodzajów przestępstw, do których są stosowane, oraz nazw przedsiębiorstw lub organizacji, które te narzędzia opracowały; wzywa organy ścigania i wymiaru sprawiedliwości do informowania opinii publicznej i zapewnienia dostatecznej przejrzystości w zakresie wykorzystywania przez nie sztucznej inteligencji i związanych z nią technologii podczas wykonywania swoich uprawnień, w tym do ujawnienia odsetka fałszywie pozytywnych i fałszywie negatywnych wskazań generowanych przez tą technologię; zwraca się do Komisji o zebranie i aktualizację informacji w jednym miejscu; wzywa Komisję do opublikowania również zaktualizowanych informacji na temat wykorzystania sztucznej inteligencji przez agencje UE, którym powierzono zadania dotyczące ścigania przestępstw i wymiaru sprawiedliwości; wzywa EROD do oceny legalności tych technologii i zastosowań sztucznej inteligencji wykorzystywanych przez organy ścigania i wymiar sprawiedliwości;

34. przypomina, że rozwiązania oparte na sztucznej inteligencji, w tym te stosowane w kontekście ścigania przestępstw i wymiaru sprawiedliwości, są obecnie opracowywane na całym świecie w szybkim tempie; wzywa wszystkie zainteresowane strony w Europie, w tym państwa członkowskie i Komisję, do zapewnienia, w drodze współpracy międzynarodowej, zaangażowania partnerów spoza UE w celu podniesienia standardów na szczeblu międzynarodowym oraz znalezienia wspólnych i uzupełniających ram prawnych i etycznych dotyczących stosowania sztucznej inteligencji, w szczególności w odniesieniu do ścigania przestępstw i do wymiaru sprawiedliwości, przy czym standardy te mają być w pełni zgodne z Kartą, europejskim dorobkiem prawnym w dziedzinie ochrony danych oraz – w szerszym ujęciu – z prawami człowieka;

35. apeluje do Agencji Praw Podstawowych Unii Europejskiej, aby we współpracy z EROD i EIOD opracowała kompleksowe wytyczne, zalecenia i najlepsze praktyki w celu doprecyzowania kryteriów i warunków opracowywania, stosowania i wdrażania aplikacji i rozwiązań sztucznej inteligencji wykorzystywanych przez organy ścigania i organy sądowe; zobowiązuje się do przeprowadzenia badania dotyczącego wdrożenia dyrektywy o ochronie danych w sprawach karnych[9] w celu określenia, w jaki sposób organy ścigania i organy sądowe zapewniły ochronę danych osobowych w trakcie przetwarzania danych, zwłaszcza przy opracowywaniu lub wdrażaniu nowych technologii; wzywa ponadto Komisję do rozważenia, czy potrzebne są konkretne działania ustawodawcze w celu doprecyzowania kryteriów i warunków opracowywania, stosowania i wdrażania aplikacji i rozwiązań sztucznej inteligencji przez organy

[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.

ścigania i organy sądowe;

36. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie i Komisji.

UZASADNIENIE

Sztuczna inteligencja jest jedną ze strategicznych technologii XXI wieku, która w znaczącym stopniu korzystnie wpływa na wydajność, dokładność i wygodę, a co za tym idzie pozytywnie przekłada się na gospodarkę europejską. Zastosowanie sztuczniej inteligencji poprawiło, między innymi, opiekę zdrowotną, zwiększyło wydajność rolnictwa, przyczyniło się do łagodzenia zmiany klimatu i do dostosowania do niej oraz poprawiło wydajność produkcji.

Sztuczna inteligencja jest jednym z najważniejszych priorytetów obecnej Komisji. W swoich wytycznych politycznych przewodnicząca Komisji, Ursula von der Leyen ogłosiła skoordynowane europejskie podejście do ludzkich i etycznych implikacji sztucznej inteligencji, jak również przemyślenia w zakresie lepszego wykorzystania dużych zbiorów danych w innowacji. Poparciu dla sztucznej inteligencji jako kwestii, którą należy rozważać na szczeblu UE, towarzyszy refleksja w zakresie tego, jak zadbać o zaufanie do technologii opartych na sztucznej inteligencji i w jaki sposób zapewnić, że nie będzie ona godzić w prawa podstawowe w UE.

Parlament Europejski zajmował się sztuczną inteligencją już kila lat zanim Komisja zdecydowała się uznać ją za ważny priorytet. Szereg rezolucji w sprawie technologii dużych zbiorów danych, robotyki i sztucznej inteligencji przyjętych przez Parlament od 2016 r. wskazuje na to, jak istotny jest ten temat dla Parlamentu. W rezolucjach przyglądnięto się różnorakim implikacjom sztucznej inteligencji oraz temu, w jaki sposób wpływa ona na dobrobyt, oświatę, technologie, kwestie prawne i prawa podstawowe, jak również szeroko rozumiany przemysł. W rezolucjach tych podkreślono potrzebę przyjęcia podejścia ukierunkowanego na człowieka, w oparciu o poszanowanie praw podstawowych, a mianowicie Karty praw podstawowych Unii Europejskiej oraz ram UE w zakresie ochrony danych.

Sztuczna inteligencja to zbiór rozwiązań technologicznych, które łączą w sobie dane, algorytmy i możliwości obliczeniowe, ponieważ kluczowym czynnikiem napędzającym obecny gwałtowny rozwój sztucznej inteligencji jest postęp w dziedzinie technologii komputerowych oraz coraz większa dostępność danych[1]. Sednem sztucznej inteligencji jest fakt, że opiera się ona na zbieraniu, analizie i okresowym gromadzeniu dużych ilości danych, w tym danych osobowych, z różnych źródeł, a dane te są następnie poddawane zautomatyzowanemu przetwarzaniu za pomocą algorytmów komputerowych i zaawansowanych technik przetwarzania danych. Techniki te korzystają zarówno ze zgromadzonych, jak i przesyłanych danych, by wygenerować zestawienia pewnych powiązań, tendencji i prawidłowości (analiza dużych zbiorów danych). Dane wykorzystywane w sztucznej inteligencji nie pochodzą jedynie od samych obywateli; aplikacje opierające się na sztucznej inteligencji głównie korzystają z przetwarzanych z wielu różnych powodów danych uzyskanych od przemysłu, przedsiębiorstw i sektora publicznego. Nawet jeżeli dane wykorzystywane przez rozwiązania oparte na sztucznej inteligencji czasami nie są danymi osobowymi, bardzo często działanie sztucznej inteligencji obejmuje przetwarzanie danych osobowych, gdyż często prowadzi ono do podejmowania zautomatyzowanych decyzji mających bezpośredni wpływ na konkretne osoby. Te właściwości sztucznej inteligencji wymagają od nas w związku z tym zwracania bacznej uwagi w tym obszarze na poszanowanie podstawowych zasad ochrony i prywatności danych.

[1] COM(2020) 65 final.

Sztuczna inteligencja oferuje również doskonałe możliwości w obszarze ścigania przestępstw oraz sądownictwa karnego, w szczególności pod względem usprawnienia metod pracy organów ścigania i władz sądowych oraz w skuteczniejszej walce z pewnymi rodzajami przestępstw, szczególnie w obszarze przestępstw finansowych, prania pieniędzy i finansowania terroryzmu oraz pewnych rodzajów cyberprzestępstw. W tym sektorze zastosowanie sztucznej inteligencji obejmuje, m.in. technologie rozpoznawania twarzy, zautomatyzowane rozpoznawanie numerów rejestracyjnych, identyfikację głosu, identyfikację sposobu mówienia, technologię czytania z ruchu warg, nasłuch (np. algorytmy wykrywające strzały), autonomiczne badanie i analizę wykrytych baz danych, przewidywanie (prognozowanie przestępczości i analityka obszarów szczególnie narażonych na przestępstwa), narzędzia wykrywania zachowań, autonomiczne narzędzia wykrywania nadużyć finansowych i finansowania terroryzmu, monitorowanie mediów społecznościowych (wyszukiwanie informacji i gromadzenie danych w celu ich eksploracji, by ustalić powiązania), urządzenia pozwalające wyłapać międzynarodowy numer tożsamości telefonicznej abonenta mobilnego (IMSI catchers) oraz zautomatyzowane systemy dozoru obejmujące różne możliwości wykrywania (takie jak wykrywanie pulsu i kamery termowizyjne). W wymiarze sprawiedliwości narzędzia oparte na sztucznej inteligencji mogą być wykorzystywane do wyliczania prawdopodobieństwa ponownego popełnienia przestępstwa oraz w ustalaniu warunków zwolnienia czy decyzji o wyroku.

Ze sztuczną inteligencją niewątpliwie wiążą się pewne korzyści, jednak faktem jest, że sztuczna inteligencja pociąga za sobą także szereg potencjalnych zagrożeń, takich jak nieprzejrzysty proces decyzyjny, różnego rodzaju dyskryminacja, naruszenie prywatności, wyzwania dla ochrony danych osobowych, ludzkiej godności oraz wolności wypowiadania się i swobody informacji. Te potencjalne zagrożenia są spotęgowane w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych, ponieważ mogą wpłynąć na domniemanie niewinności, prawa podstawowe do wolności i bezpieczeństwa osób oraz do skutecznego środka odwoławczego i sprawiedliwego procesu.

Celem niniejszego sprawozdania jest zajęcie się kwestiami wynikającymi z wykorzystania sztucznej inteligencji w prawie karnym oraz korzystania z niej przez policję i wymiar sprawiedliwości w sprawach karnych. Należy przyznać, że sztuczna inteligencja może przynieść potencjalne szanse i korzyści, jednak należy również podkreślić znaczące zagrożenia i konsekwencje z nią związane.

W niniejszym sprawozdaniu podkreślono potrzebę pełnego poszanowania praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej, unijnym prawie w zakresie ochrony prywatności i danych, a mianowicie dyrektywie (UE) 2016/680 (dyrektywa policyjna) oraz konieczność wdrożenia szeregu kluczowych zasad w cyklu życia sztucznej inteligencji, takich jak możliwość wyjaśnienia zasad funkcjonowania algorytmu oraz przejrzystość, możliwość ustalenia faktów, przeprowadzanie obowiązkowych analiz skutków sztucznej inteligencji dla praw podstawowych przed wdrożeniem lub rozpoczęciem stosowania wszelkich systemów sztucznej inteligencji oraz obowiązkowe audyty. Spełnienie wszystkich tych wymogów jest nie tylko konieczne, by zagwarantować legalność systemów sztucznej inteligencji, lecz również by zaskarbić sobie zaufanie obywateli do wykorzystania systemów sztucznej inteligencji przez organy ścigania i organy wymiaru sprawiedliwości w sprawach karnych.

Na zakończenie sprawozdawca wzywa do przyjęcia moratorium na wdrożenie systemów rozpoznawania twarzy dla celów ścigania. Bieżący stan rozwoju tych technologii i ich poważny wpływ na prawa podstawowe wymaga dogłębnej i otwartej debaty społecznej, by pochylić się nad różnorodnymi kwestiami i nad uzasadnieniem wdrożenia takich systemów.

3.9.2020

OPINIA KOMISJI RYNKU WEWNĘTRZNEGO I OCHRONY KONSUMENTÓW

dla Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych
(2020/2016(INI))

Sprawozdawca komisji opiniodawczej: Marcel Kolaja

WSKAZÓWKI

Komisja Rynku Wewnętrznego i Ochrony Konsumentów zwraca się do Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, jako komisji przedmiotowo właściwej, o uwzględnienie w końcowym tekście projektu rezolucji następujących wskazówek:

A. mając na uwadze, że w świetle pozytywnego potencjału społecznego sztucznej inteligencji (SI) i związanych z nią nieodłącznie zagrożeń należy poprawić funkcjonowanie jednolitego rynku cyfrowego, zapewniając podmiotom oferującym systemy SI większą pewność prawa i zwiększając zaufanie i bezpieczeństwo użytkowników przez wzmocnienie zabezpieczeń, aby zagwarantować praworządność i przestrzeganie praw podstawowych, w szczególności prawa do prywatności i ochrony danych osobowych, prawa do równości i niedyskryminacji, prawa do dobrej administracji, rzetelnego procesu sądowego i wysokiego poziomu ochrony konsumenta; mając na uwadze, że wspólne europejskie podejście do sztucznej inteligencji i uregulowania jej stosowania w sprawach karnych przez policję i organy ścigania jest konieczne, aby uniknąć rozdrobnienia jednolitego rynku;

B. mając na uwadze, że testowanie i wykorzystywanie SI przez policję i organy wymiaru sprawiedliwości jest powszechne, co wiąże się z różnego rodzaju zastosowaniami, konsekwencjami i zagrożeniami, a mianowicie systemami rozpoznawania twarzy, profilowaniem DNA, prognozowaniem map przestępczości, pobieraniem danych z telefonów komórkowych, zaawansowanymi wyszukiwarkami orzecznictwa, internetowym rozstrzyganiem sporów oraz uczeniem się maszyn na potrzeby sprawowania wymiaru sprawiedliwości;

C. mając na uwadze, że stosowanie sztucznej inteligencji może stanowić zmianę paradygmatu sprawowania wymiaru sprawiedliwości w sprawach karnych;

D. mając na uwadze, że zgodnie ze sprawozdaniem Agencji Praw Podstawowych nadal dostępne są obecnie jedynie ograniczone informacje na temat możliwego zastosowania

lub testowania technologii rozpoznawania twarzy w państwach członkowskich[1];

E. mając na uwadze, że w państwach członkowskich, w których dostępne były pewne informacje na temat zastosowania technologii rozpoznawania twarzy, organy ochrony danych ustaliły, że wykorzystanie tych technologii nie było zgodne z przepisami w zakresie ochrony danych osobowych i brakowało podstawy prawnej do ich wdrożenia;

F. mając na uwadze, że reformując procedury udzielania zamówień publicznych, Unia może mieć w obszarze rynku wewnętrznego znaczący wpływ na dostosowanie działań i zachowań rządów do drugorzędnych celów polityki, takich jak ochrona danych i niedyskryminacja;

G. mając na uwadze, że w wyniku błędów nielosowych w zbiorach danych lub algorytmach na etapie projektowania, testowania i wdrażania może dojść do dyskryminacji w algorytmicznym procesie decyzyjnym opartym na danych;

H. mając na uwadze, że techniczne opracowanie i stosowanie sztucznej inteligencji w oparciu o zasady jest konieczne, aby zapewnić zgodność z prawami człowieka i prawami podstawowymi;

I. mając na uwadze, że 4 grudnia 2018 r. Europejska Komisja na rzecz Efektywności Wymiaru Sprawiedliwości Rady Europy opublikowała Kartę etyki dotyczącą stosowania sztucznej inteligencji na potrzeby wymiaru sprawiedliwości, w której określono etyczne zasady wykorzystania sztucznej inteligencji na potrzeby wymiaru sprawiedliwości;

J. mając na uwadze, że niektóre zastosowania technologii SI są szczególnie wrażliwe i podatne na nadużycia, przez co w ostatnim czasie niektóre przedsiębiorstwa technologiczne podjęły decyzję o zaprzestaniu oferowania odnośnego oprogramowania;

1. uważa, że sztuczną inteligencję wykorzystywaną przez policję i organy wymiaru sprawiedliwości trzeba uznać za charakteryzującą się wysokim ryzykiem i traktować z maksymalną uwagą oraz zgodnie z najwyższymi standardami ochrony danych z uwagi na rolę tych organów polegającą na obronie interesu publicznego i na charakter ich zadań; uważa, że należy pilnie stworzyć wspólne europejskie ramy regulujące SI na rynku wewnętrznym; uważa, że UE powinna odgrywać wiodącą rolę w opracowywaniu regulacji na szczeblu Unii, w tym dotyczących zamówień publicznych, w oparciu o jasne zasady, prawa podstawowe i etykę, w opracowywaniu i stosowaniu SI, aby zapewnić taki sam wysoki poziom ochrony konsumentów i jednolite normy przemysłowe w całej UE oraz usprawnić funkcjonowanie rynku wewnętrznego, a jednocześnie zachęcać do innowacji i zwiększać pewność prawa dla przedsiębiorstw, zwłaszcza MŚP; wzywa Komisję, aby szczegółowo zbadała stosowanie obowiązującego prawodawstwa i jego egzekwowanie przed wystąpieniem z możliwymi nowymi wnioskami ustawodawczymi;

[1] Agencja Praw Podstawowych Unii Europejskiej: Technologia rozpoznawania twarzy: kwestie związane z prawami podstawowymi w kontekście egzekwowania prawa (FRA Focus), 27 listopada 2019 r. – https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

2. uznaje, że stosowanie SI w obszarze wymiaru sprawiedliwości może się przyczynić do poprawy wydajności i jakości postępowań; podkreśla w tym kontekście, że w szczególności konieczne jest przestrzeganie zasad określonych w europejskiej konwencji praw człowieka i Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych;

3. wzywa Komisję do dokonania oceny technologii sztucznej inteligencji dostępnej na rynku oraz stopnia jej wykorzystania przez policję i organy wymiaru sprawiedliwości w poszczególnych państwach.

4. podkreśla, że sztuczna inteligencja powinna przyczynić się do zmniejszenia obciążeń administracyjnych spoczywających na organach publicznych i do zwiększenia wydajności ich procesu decyzyjnego oraz że systemy sztucznej inteligencji powinny opierać się na ludzkiej kontroli, współpracy i koordynacji; w związku z tym podkreśla, że ludzie powinni zawsze ponosić ostateczną odpowiedzialność za wszelkie decyzje w sprawach karnych; podkreśla znaczenie dokładnych zbiorów danych, jeżeli są one wykorzystywane do wspomagania powiązanych procesów administracji elektronicznej i podejmowania decyzji administracyjnych w całej Unii;

5. podkreśla znaczenie wspierania innowacji, przejrzystości, identyfikowalności i weryfikacji; podkreśla, że SI oparta na otwartym oprogramowaniu mogłaby się do tego przyczynić, jednocześnie wzmacniając też współpracę oraz kulturę wymiany pomysłów i doświadczeń związanych z wykorzystywaniem i tworzeniem algorytmów;

6. uważa, że sztuczną inteligencję wykorzystywaną przez policję i organy ścigania w sprawach karnych należy udostępniać jako otwarte oprogramowanie w miarę możliwości w ramach procedury udzielania zamówień publicznych zgodnie z obowiązującym prawodawstwem, w tym z dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym, przy czym dokumentacja oprogramowania i algorytmy powinny być dostępne, co umożliwi właściwym organom ustalenie, w jaki sposób system SI doszedł do pewnego wniosku; podkreśla, że kontrola przestrzegania praw podstawowych powinna być częścią wcześniejszej oceny zgodności; uważa, że przy zapewnianiu przestrzegania prawa i wartości UE oraz obowiązujących przepisów o ochronie danych, bez narażania dobra śledztw czy postępowań karnych, zrozumiałe i obiektywne algorytmy, które spełniają wymóg wystarczającej przejrzystości, a także wykorzystywanie otwartych danych do celów szkoleniowych zgodnie z dyrektywą (UE) 2019/1024 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego, nie naruszając rozporządzenia (UE) 2016/679, mają zasadnicze znaczenie dla zapewnienia, by przedsiębiorstwa i obywatele, w tym konsumenci, mogli mieć zaufanie do lepszych, dostępnych, niedyskryminacyjnych i niezawodnych usług publicznych oraz czerpać z nich korzyści po sprawiedliwych kosztach;

7. podkreśla, że gromadzenie danych opartych na SI i monitorowanie osób powinno ograniczać się do podejrzanych o popełnienie przestępstwa i nadzoru zatwierdzonego przez sąd zgodnie z obowiązującym prawem krajowym, z uwzględnieniem poszanowania życia prywatnego i domniemania niewinności, w tym innych użytkowników i konsumentów, na których takie systemy i praktyki mogą mieć przypadkowo wpływ; podkreśla, że w przypadkach gdy proces decyzyjny wspomagają

obliczenia statystyczne, osoby podejmujące decyzje powinny posiadać odpowiednie przeszkolenie zawodowe i kwalifikacje w kwestii potencjału stronniczości, ponieważ zbiory danych mogą zawierać dane oparte na dyskryminacji i uprzedzeniach; podkreśla w związku z tym znaczenie jakości algorytmów i danych pierwotnych oraz przypomina, że stosowanie sztucznej inteligencji musi opierać się na zasadzie niedyskryminacji przy wprowadzaniu i analizie danych; apeluje, aby procedury udzielania zamówień na takie zastosowania zawierały zabezpieczenia przed ewentualnymi błędami nielosowymi; wzywa do wymiany informacji i najlepszych praktyk dotyczących stosowania technik i narzędzi SI przez organy sądowe i policyjne w państwach członkowskich, aby uniknąć fragmentarycznego podejścia na jednolitym rynku i zapewnić ochronę konsumentów i obywateli w całej Unii;

8. uważa, że zgodnie z obowiązującymi przepisami prawa karnego państwa członkowskie powinny dopilnować, aby obywatele i konsumenci byli informowani, kiedy wobec nich stosowana jest sztuczna inteligencja, oraz aby obywatele mieli dostęp do prostych, skutecznych i łatwo dostępnych procedur wnoszenia skarg i dochodzenia roszczeń, w tym sądowych środków odwoławczych, umożliwiających skuteczną obronę swoich praw;

9. przypomina, że z niektórymi rodzajami SI wiąże się duże ryzyko, np. z technologiami rozpoznawania twarzy w przestrzeni publicznej, automatycznym wykrywaniem zachowań i profilowaniem w celu dzielenia ludzi na kategorie ryzyka na granicach, wykrywaniem biometrycznym i biometrią na potrzeby masowej inwigilacji, oceną punktową obywateli na masową skalę i prognozowaniem przestępczości, oraz wzywa Komisję, aby uregulowała ich zamawianie i stosowanie w celu wyeliminowania ryzyka nadużyć; pod tym względem przyjmuje z zadowoleniem trwające prace Komisji nad oceną wykorzystania technologii biometrycznych i jej rozważania dotyczące wariantów regulacyjnych, w tym podejścia opartego na ryzyku, zakazu stosowania tych technologii w pewnych okolicznościach oraz wprowadzenia koniecznych zabezpieczeń tam, gdzie zastosowanie tych technologii jest uzasadnione;

10. podkreśla, że w celu uniknięcia standaryzacji decyzji w oparciu o obliczenia czysto statystyczne należy utrzymać suwerenną swobodę decyzyjną sędziów i podejmowanie decyzji w indywidualnych przypadkach.

INFORMACJE O PRZYJĘCIU PRZEZ KOMISJĘ OPINIODAWCZĄ

Data przyjęcia	3.9.2020
Wynik głosowania końcowego	+: 40 –: 4 0: 0
Posłowie obecni podczas głosowania końcowego	Alex Agius Saliba, Andrus Ansip, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Dita Charanzová, Deirdre Clune, David Cormand, Petra De Sutter, Carlo Fidanza, Evelyne Gebhardt, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Adriana Maldonado López, Antonius Manders, Beata Mazurek, Leszek Miller, Dan-Ştefan Motreanu, Kris Peeters, Anne-Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann, Marco Zullo
Zastępcy obecni podczas głosowania końcowego	Maria da Graça Carvalho, Anna Cavazzini, Krzysztof Hetman

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI OPINIODAWCZEJ

40	+
PPE	Maria da Graça Carvalho, Deirdre Clune, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Dan-Ştefan Motreanu, Kris Peeters, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
S&D	Alex Agius Saliba, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Adriana Maldonado López, Leszek Miller, Christel Schaldemose
RENEW	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Svenja Hahn, Morten Løkkegaard
ID	Hynek Blaško
VERTS/ALE	Anna Cavazzini, David Cormand, Petra De Sutter, Marcel Kolaja, Kim Van Sparrentak
ECR	Adam Bielan, Carlo Fidanza, Eugen Jurzyca, Beata Mazurek
GUE/NGL	Kateřina Konečná, Anne-Sophie Pelletier
NI	Marco Zullo

4	-
ID	Alessandra Basso, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle

0	0

Objaśnienie używanych znaków:
+ : za
- : przeciw
0 : wstrzymało się

15.9.2020

OPINIA KOMISJI PRAWNEJ

dla Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych
(2020/2016(INI))

Sprawozdawca komisji opiniodawczej: Angel Dzhambazki

WSKAZÓWKI

Komisja Prawna zwraca się do Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, jako komisji przedmiotowo właściwej, o uwzględnienie w końcowym tekście projektu rezolucji następujących wskazówek:

A. mając na uwadze, że podczas egzekwowania prawa prawo do rzetelnego procesu sądowego jest prawem podstawowym i prawnie wiążącym wynikającym z Karty praw podstawowych Unii Europejskiej i europejskiej konwencji praw człowieka; mając na uwadze, że ma ono zastosowanie przez cały czas trwania postępowania karnego, w tym w kontekście egzekwowania prawa, a jego poszanowanie na wszystkich etapach postępowania wyklucza podejmowanie środków, w tym środków technicznych, których bezpośrednim lub pośrednim skutkiem byłoby naruszenie istoty prawa do obrony; mając na uwadze, że gwarancje związane z tą zasadą, w szczególności gwarancje „niezależnego sądu", „równości wobec prawa" i „domniemania niewinności", są bardziej rygorystyczne w prawie karnym; mając na uwadze, że praw tych należy przestrzegać w każdych okolicznościach, w szczególności podczas stosowania sztucznej inteligencji (SI), zwłaszcza biorąc pod uwagę fakt, że technologie oparte na sztucznej inteligencji mogą mieć wpływ na różne prawa człowieka;

B. mając na uwadze, że ochrona danych osobowych, zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO)[1] i, w stosownym przypadku, z innymi właściwymi przepisami, ma zastosowanie w każdych okolicznościach;

C. mając na uwadze, że sztuczna inteligencja i powiązane z nią technologie, w tym ich zdolność do samouczenia się, w każdym przypadku wiążą się z pewnym stopniem interwencji człowieka;

D. mając na uwadze, że sztuczna inteligencja może stać się stałym elementem systemów

[1] 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 (Dz.U. L 119 z 4.5.2016, s. 1).

prawa karnego;

E. mając na uwadze, że sztuczna inteligencja i powiązane z nią technologie są dla UE priorytetem ze względu na szybki postęp w sektorze technologicznym oraz znaczenie zachowania czujności w odniesieniu do ich obecnego i przyszłego wpływu na jednolity europejski system praw własności intelektualnej; mając na uwadze, że sztuczna inteligencja i powiązane z nią technologie już są wdrażane w różnych sektorach, np. w robotyce, transporcie i służbie zdrowia, by wymienić tylko kilka z nich;

F. mając na uwadze, że technologie takie jak sztuczna inteligencja i powiązane z nią technologie mogłyby być wykorzystywane w dziedzinie prawa karnego w celu obniżenia wskaźnika przestępczości, ułatwienia niektórych procedur poprzez ich wykorzystanie w analizie danych statystycznych w dziedzinie analizy przestępczości i zapobiegania jej, a także w celu wykrywania i prowadzenia dochodzeń w sprawach karnych; mając na uwadze, że Unia powinna dalej rozwijać swoje zdolności w zakresie oprogramowania, przechowywania danych i technologii sztucznej inteligencji w celu osiągnięcia poprawy, jeśli chodzi o niedociągnięcia w zakresie ochrony danych i prywatności;

G. mając na uwadze, że technologie te mogą być wykorzystywane do tworzenia anonimowych, statystycznych baz danych, które ułatwią organom władzy, pracownikom akademickim i ustawodawcom analizę danych liczbowych i skuteczne opracowywanie strategii zapobiegania przestępczości oraz pomaganie przestępcom w ich resocjalizacji;

H. mając na uwadze, że ramy prawne dotyczące sztucznej inteligencji i jej zastosowania w prawie karnym powinny – jeżeli istnieje taka konieczność – obejmować działania ustawodawcze, począwszy od obowiązkowych środków mających na celu zapobieganie praktykom, które w sposób niebudzący wątpliwości podważają podstawowe prawa i wolności;

I. mając na uwadze, że – ze względu na z natury nieprzejrzysty charakter systemów sztucznej inteligencji – nowe narzędzia stosowane w sądownictwie karnym mogą być sprzeczne z niektórymi podstawowymi wolnościami;

J. mając na uwadze, że należy zapobiegać potencjalnym zagrożeniom związanym ze stosowaniem systemów sztucznej inteligencji w sądownictwie karnym i zmniejszać te zagrożenia w celu ochrony praw podstawowych osób podejrzanych i oskarżonych w postępowaniu karnym;

1. podkreśla zasadnicze znaczenie należytej oceny zagrożeń, takich jak dyskryminacja i prywatność, związanych ze stosowaniem systemów sztucznej inteligencji oraz uwzględnienia wszystkich etycznych i operacyjnych skutków stosowania sztucznej inteligencji i powiązanych z nią technologii w naszym społeczeństwie, w szczególności ze strony organów krajowych, policji i organów wymiaru sprawiedliwości w systemach sądownictwa karnego, a także kwestii związanych z odpowiedzialnością i ciężarem dowodowym w przypadku potencjalnych błędów związanych z funkcjonowaniem systemów sztucznej inteligencji; uważa, że potrzebne są jasne ramy regulacyjne, aby wyznaczyć granice i zapewnić niezbędne zabezpieczenia; uważa, że należy wziąć pod uwagę zasady etyczne, takie jak te określone w przyjętej przez Radę Europy

Europejskiej karcie etycznej dotyczącej stosowania sztucznej inteligencji w systemach sądownictwa karnego i środowiskach pokrewnych oraz że podmioty publiczne i prywatne odpowiedzialne za pierwotny projekt oraz za rozwój narzędzi i usług opartych na sztucznej inteligencji powinny przestrzegać tej karty, tak aby wszystkie odpowiednie podmioty społeczne dysponowały wyczerpującymi informacjami na temat struktury organizacyjnej przedsiębiorstw wytwarzających programy sztucznej inteligencji; podkreśla znaczenie czynnika ludzkiego, który zawsze musi być ostatecznym decydentem w sprawie korzystania z oprogramowania opartego na technologiach sztucznej inteligencji w systemie sądownictwa karnego, zarówno w odniesieniu do egzekwowania prawa przez policję, jak i do sądownictwa karnego; przypomina, że oprogramowanie do rozpoznawania biometrycznego powinno być stosowane wyłącznie w przypadkach, gdy jest to wyraźnie uzasadnione;

2. podkreśla potrzebę ustanowienia i utrzymania równowagi między wykorzystywaniem systemów sztucznej inteligencji w postępowaniach karnych a poszanowaniem wszystkich praw podstawowych i gwarancji proceduralnych przewidzianych w prawie europejskim i międzynarodowym;

3. podkreśla znaczenie stosowania sztucznej inteligencji z należytym poszanowaniem zasad praworządności i niezależności sądów w procesie podejmowania decyzji;

4. wzywa Komisję do dalszego doprecyzowania przepisów dotyczących ochrony i udostępniania danych zgromadzonych z wykorzystaniem sztucznej inteligencji i powiązanych z nią technologii przez organy uprawnione do ich gromadzenia lub przetwarzania, w tym danych nieosobowych i zanonimizowanych, które bezpośrednio lub pośrednio identyfikują osoby fizyczne, przy pełnym poszanowaniu przepisów RODO i dyrektywy o prywatności i łączności elektronicznej[2]; podkreśla ponadto, że prawo do rzetelnego procesu sądowego powinno obejmować prawo dostępu obywateli i osób uczestniczących w postępowaniu sądowym do tych danych, zwłaszcza gdy są one gromadzone z ich osobistych urządzeń lub sprzętu, zgodnie z RODO, ale także w celu skorzystania z prawa do obrony w przypadku pociągnięcia ich do odpowiedzialności prawnej;

5. podkreśla znaczenie zwiększenia przejrzystości systemów opartych na sztucznej inteligencji wykorzystywanych w sprawach karnych w celu umożliwienia nadzoru sądowego oraz zagwarantowania, że podmioty opracowujące sztuczną inteligencję i powiązane z nią technologie zapewniają wystarczający poziom przejrzystości algorytmów i decyzji algorytmicznych w interesie właściwych organów i obywateli; podkreśla ogólne prawo stron do uzyskania dostępu do procesów związanych z gromadzeniem danych, ocenami prognostycznymi stosowanymi do celów zapobiegania przestępczości, katalogowaniem i oceną dowodów karnych oraz określaniem, czy podejrzany może stanowić zagrożenie dla społeczeństwa, jeżeli nie jest ograniczony obowiązującym prawem UE, takim jak dyrektywa (UE) 2016/680[3]; podkreśla ponadto

[2] 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 (Dz.U. L 201 z 31.7.2002, s. 37).
[3] 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 (Dz.U. L 119 z 4.5.2016, s. 89).

znaczenie dostępu do wyników osiąganych lub wspomaganych przez sztuczną inteligencję oraz ostatecznego określenia odpowiedzialności za procedury powiadamiania i roli sztucznej inteligencji i powiązanych z nią technologii w sprawach karnych, w szczególności w odniesieniu do analizy znacznych ilości dowodów w dochodzeniach karnych oraz identyfikacji podejrzanych lub ofiar przestępstw; przypomina o znaczeniu kwestii związanych z zarządzaniem, prawami podstawowymi i gwarancjami proceduralnymi, niedyskryminacją, rozliczalnością, przejrzystością, bezstronnością, sprawiedliwością i intelektualną integralnością sztucznej inteligencji i powiązanych z nią technologii i podkreśla jednocześnie potrzebę zapewnienia stałego nadzoru ze strony człowieka; podkreśla, że organy wymiaru sprawiedliwości muszą być zobowiązane do uzasadniania swoich decyzji, w tym w przypadkach, gdy opierają się one na dowodach pochodzących z technologii wspomaganych przez sztuczną inteligencję, które muszą podlegać skrupulatnej kontroli sądowej i których dopuszczalność nie powinna budzić wątpliwości, zgodnie z rezolucją z dnia 16 lutego 2017 r. w sprawie robotyki[4], w której podkreślono, że w każdym przypadku powinno być możliwe uzasadnienie wszelkich decyzji podjętych z wykorzystaniem sztucznej inteligencji, mogących mieć istotny wpływ na życie przynajmniej jednej osoby; przypomina o rozróżnieniu między wykorzystaniem sztucznej inteligencji i powiązanych z nią technologii w zapobieganiu przestępczości oraz w systemach sądownictwa karnego; podkreśla, że technologie sztucznej inteligencji muszą zawsze pełnić podrzędną rolę;

6. przypomina, że najpoważniejsze przypadki niewłaściwego wykorzystania sztucznej inteligencji i powiązanych z nią technologii, takie jak masowa inwigilacja, profilowanie, programy prognozowania przestępczości, które mogłyby służyć do oceny prawdopodobnego miejsca popełnienia przestępstwa, możliwej lokalizacji podejrzanych, prawdopodobieństwa wiktymizacji danej osoby, jej podatności na zagrożenia, jej zaginięcia lub stania się ofiarą lub sprawcą przemocy domowej lub przestępstwa na tle seksualnym, a także naruszenia należnych praw procesowych mogą wynikać z działań organów publicznych odpowiedzialnych za egzekwowanie prawa;

7. podkreśla znaczenie wykorzystywania automatycznie generowanych danych przy gromadzeniu i analizie dowodów; przypomina, że w zapobieganiu przestępczości i w systemach sądownictwa karnego błędy w analizie wprowadzonych i wytworzonych danych lub możliwego niewłaściwego wykorzystania danych w tej analizie można przypisać czynnikowi ludzkiemu, w związku z tym wzywa do przyjęcia ostrożnego podejścia podczas analizy skuteczności i przydatności stosowania technologii opartych na sztucznej inteligencji we wszystkich procesach decyzyjnych;

8. wzywa wszystkie właściwe organy publiczne, w szczególności organy egzekwowania prawa, takie jak policja i wymiar sprawiedliwości, do informowania opinii publicznej i zapewniania dostatecznej przejrzystości w zakresie wykorzystywania przez nie sztucznej inteligencji i powiązanych z nią technologii podczas wykonywania swoich uprawnień, zwłaszcza w sprawach karnych;

9. uznaje za konieczne, by stosowanie systemów sztucznej inteligencji w postępowaniu karnym gwarantowało poszanowanie podstawowych zasad postępowania karnego, w

[4] Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (Dz.U. C 252 z 18.7.2018, s. 239).

tym prawa do rzetelnego procesu sądowego, zasady domniemania niewinności oraz prawa do skutecznego środka prawnego, przy jednoczesnym zapewnieniu niezależnego monitorowania i kontroli systemów zautomatyzowanego podejmowania decyzji;

10. podkreśla znaczenie zasady ludzkiej kontroli oraz weryfikacji wyników wytworzonych przez sztuczną inteligencję lub uzyskanych z jej wykorzystaniem; przypomina również o znaczeniu zarządzania, przejrzystości, wyjaśnialności i rozliczalności dla zapewnienia poszanowania praw podstawowych i unikania potencjalnych błędów w działaniu sztucznej inteligencji;

11. podkreśla swoje ostrożne podejście do korzystania z oprogramowania do rozpoznawania biometrycznego; podkreśla niejednoznaczność wynikającą z inherentnych niedoskonałości, jeśli chodzi o ochronę danych, a także naruszeń prywatności danych; z niepokojem odnotowuje gromadzenie danych osobowych dotyczących obywateli w Unii Europejskiej przez państwa trzecie za pośrednictwem programistów i dostawców z sektora prywatnego;

12. przypomina, że zgodnie z obowiązującymi przepisami UE o ochronie danych oraz z Kartą praw podstawowych Unii Europejskiej sztuczna inteligencja może być wykorzystywana do zdalnej identyfikacji biometrycznej wyłącznie wtedy, gdy jest to należycie uzasadnione, proporcjonalne i objęte odpowiednimi zabezpieczeniami; z zadowoleniem przyjmuje zalecenia powołanej przez Komisję grupy ekspertów wysokiego szczebla ds. AI dotyczące proporcjonalnego, ostrożnego i opartego na analizie ryzyka wykorzystania technologii biometrycznych, zgodnie z przepisami dotyczącymi ochrony danych osobowych; sugeruje, że stosowanie tych technologii musi być wyraźnie uzasadnione w ramach obowiązującego prawa i sugeruje, aby Komisja dokonała oceny sposobów skutecznego włączenia tych zaleceń, ze szczególnym uwzględnieniem prawa do prywatności i ochrony danych osobowych;

13. wyraża głębokie przekonanie, że decyzje podejmowane przez sztuczną inteligencję lub powiązane z nią technologie, szczególnie w dziedzinie wymiaru sprawiedliwości i egzekwowania prawa, i mające bezpośredni i istotny wpływ na prawa i obowiązki osób fizycznych lub prawnych, powinny podlegać ścisłej weryfikacji przez człowieka i odpowiednim procedurom;

14. uważa, że należy przeanalizować, czy wskazane jest częściowe powierzanie sztucznej inteligencji decyzji dotyczących egzekwowania prawa, a jeśli tak, to na jakich warunkach i w jakim zakresie można zezwolić na stosowanie sztucznej inteligencji; uważa, że sztuczna inteligencja i powiązane z nią technologie, które mogą zastąpić decyzje organów publicznych, powinny być traktowane z najwyższą ostrożnością; podkreśla potrzebę opracowania ścisłych zasad etycznych i szczegółowych kodeksów postępowania dotyczących projektowania i stosowania sztucznej inteligencji, aby pomóc organom odpowiedzialnym za egzekwowanie prawa i organom wymiaru sprawiedliwości w przypadkach, gdy decyzje dotyczące egzekwowania prawa są powierzone sztucznej inteligencji; odnosi się do bieżących prac Komisji Prawnej.

INFORMACJE O PRZYJĘCIU PRZEZ KOMISJĘ OPINIODAWCZĄ

Data przyjęcia	10.9.2020
Wynik głosowania końcowego	+: 22 –: 3 0: 0
Posłowie obecni podczas głosowania końcowego	Manon Aubry, Gunnar Beck, Geoffroy Didier, Angel Dzhambazki, Ibán García Del Blanco, Jean-Paul Garraud, Esteban González Pons, Mislav Kolakušić, Gilles Lebreton, Karen Melchior, Jiří Pospíšil, Franco Roberti, Marcos Ros Sempere, Liesje Schreinemacher, Stéphane Séjourné, Raffaele Stancanelli, Marie Toussaint, Adrián Vázquez Lázara, Axel Voss, Marion Walsmann, Tiemo Wölken, Lara Wolters, Javier Zarzalejos
Zastępcy obecni podczas głosowania końcowego	Heidi Hautala, Emil Radev

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI OPINIODAWCZEJ

22	+
PPE	Geoffroy Didier, Esteban González Pons, Jiří Pospíšil, Emil Radev, Axel Voss, Marion Walsmann, Javier Zarzalejos
S&D	Ibán García Del Blanco, Franco Roberti, Marcos Ros Sempere, Tiemo Wölken, Lara Wolters
RENEW	Karen Melchior, Liesje Schreinemacher, Stéphane Séjourné, Adrián Vázquez Lázara
ID	Gunnar Beck, Jean-Paul Garraud, Gilles Lebreton
ECR	Angel Dzhambazki, Raffaele Stancanelli
NI	Mislav Kolakušić

3	-
VERTS/ALE	Heidi Hautala, Marie Toussaint
GUE/NGL	Manon Aubry

0	0

Objaśnienie używanych znaków:
+ : za
- : przeciw
0 : wstrzymało się

INFORMACJE O PRZYJĘCIU PRZEZ KOMISJĘ PRZEDMIOTOWO WŁAŚCIWĄ

Data przyjęcia	29.6.2021
Wynik głosowania końcowego	+: 36 –: 24 0: 6
Posłowie obecni podczas głosowania końcowego	Magdalena Adamowicz, Konstantinos Arvanitis, Malik Azmani, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Jean-Paul Garraud, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Fabienne Keller, Peter Kofod, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Dragoş Tudorache, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Elena Yoncheva, Javier Zarzalejos
Zastępcy obecni podczas głosowania końcowego	Tanja Fajon, Miguel Urbán Crespo

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI PRZEDMIOTOWO WŁAŚCIWEJ

36	**+**
NI	Laura Ferrara, Martin Sonneborn
Renew	Malik Azmani, Anna Júlia Donáth, Sophia in ‘t Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Łukasz Kohut, Juan Fernando López Aguilar, Javier Moreno Sánchez, Birgit Sippel, Bettina Vollath, Elena Yoncheva
The Left	Konstantinos Arvanitis, Pernando Barrena Arza, Cornelia Ernst, Miguel Urbán Crespo
Verts/ALE	Patrick Breyer, Saskia Bricmont, Damien Carême, Alice Kuhnke, Terry Reintke, Diana Riba i Giner, Tineke Strik
24	**-**
ID	Nicolas Bay, Nicolaus Fest, Jean-Paul Garraud, Marcel de Graaff, Peter Kofod, Annalisa Tardino, Tom Vandendriessche
NI	Milan Uhrík
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Andrzej Halicki, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Tomas Tobé, Elissavet Vozemberg-Vrionidi, Javier Zarzalejos
6	**0**
ECR	Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Patryk Jaki, Nicola Procaccini, Jadwiga Wiśniewska
PPE	Emil Radev

Objaśnienie używanych znaków:
+ : za
- : przeciw
0 : wstrzymało się