Środa, 6 października 2021 r.

P9_TA(2021)0405

Sztuczna inteligencja w prawie karnym i jej stosowanie przez policję i organy wymiaru sprawiedliwości w sprawach karnych

Rezolucja Parlamentu Europejskiego z dnia 6 października 2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych (2020/2016(INI))

(2022/C 132/02)

Parlament Europejski,

— uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 2 i 6, oraz Traktat o funkcjonowaniu Unii Europejskiej, 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 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]),

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

— 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 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;

([5]) Dz.U. L 135 z 24.5.2016, s. 53.
([6]) Dz.U. C 362 z 8.9.2021, s. 63.
([7]) Dz.U. C 263 z 25.7.2018, s. 82.

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; 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;

([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).

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 ścigania i organy sądowe;

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

([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).