Wtorek, 14 marca 2017 r.

P8_TA(2017)0076

Wpływ technologii dużych zbiorów danych na prawa podstawowe

Rezolucja Parlamentu Europejskiego z dnia 14 marca 2017 r. w sprawie wpływu technologii dużych zbiorów danych na prawa podstawowe: prywatność, ochrona danych, niedyskryminacja, bezpieczeństwo i ściganie przestępstw (2016/2225(INI))

(2018/C 263/10)

Parlament Europejski,

— uwzględniając art. 16 Traktatu o funkcjonowaniu Unii Europejskiej,

— uwzględniając art. 1, 7, 8, 11, 14, 21, 47 i 52 Karty praw podstawowych Unii Europejskiej,

— uwzględniając opracowane przez Zgromadzenie Ogólne Narodów Zjednoczonych wytyczne dotyczące regulacji odnoszących się do elektronicznych banków danych, zawarte w rezolucji 45/95 z dnia 14 grudnia 1990 r.,

— 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]), a także 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 komunikat Komisji z dnia 6 maja 2015 r. dla Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, zatytułowany „Strategia jednolitego rynku cyfrowego dla Europy" (COM(2015)0192),

— uwzględniając konwencję Rady Europy nr 108 z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108) oraz protokół dodatkowy do tej konwencji z dnia 8 listopada 2001 r. (ETS nr 181) ([3]),

— uwzględniając zalecenie Komitetu Ministrów Rady Europy CM/Rec(2010)13 dla państw członkowskich o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania, przyjęte w dniu 23 listopada 2010 r. ([4]),

— uwzględniając opinię Europejskiego Rzecznika Ochrony Danych nr 7/2015 z dnia 19 listopada 2015 r. pt. „Podjęcie wyzwań związanych z dużymi zbiorami danych – apel o przejrzystość, kontrolę nad użytkownikami, ochronę danych w fazie projektowania i rozliczalność" ([5]),

— uwzględniając opinię Europejskiego Inspektora Ochrony Danych nr 8/2016 z dnia 23 września 2016 r. pt. „Opinia EIOD w sprawie spójnego egzekwowania praw podstawowych w epoce dużych zbiorów danych" ([6]),

([1]) Dz.U. L 119 z 4.5.2016, s. 1.
([2]) Dz.U. L 119 z 4.5.2016, s. 89.
([3]) http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
([4]) https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00
([5]) https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf
([6]) https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-09-23_BigData_opinion_EN.pdf

— uwzględniając oświadczenie Grupy Roboczej ds. Ochrony Danych Art. 29 z dnia 16 września 2014 r. w sprawie wpływu rozwijania dużych zbiorów danych na ochronę osób w związku z przetwarzaniem ich danych osobowych w UE ([1]),

— uwzględniając art. 52 Regulaminu,

— uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (A8-0044/2017),

A. mając na uwadze, że termin „duże zbiory danych" odnosi się do zbierania, analizy i stałego gromadzenia dużych ilości danych, w tym danych osobowych, z przeróżnych źródeł, które są automatycznie przetwarzane za pomocą algorytmów komputerowych oraz zaawansowanych technik przetwarzania danych, wykorzystujących zarówno dane zapisane, jak i przesyłane strumieniowo, aby ustalić pewne korelacje, tendencje i wzorce (analiza dużych zbiorów danych);

B. mając na uwadze, że niektóre przypadki użycia dużych zbiorów danych obejmują szkolenie urządzeń sztucznej inteligencji, takich jak sieci neuronowe i modele statystyczne, w celu przewidywania pewnych zdarzeń i zachowań; mając na uwadze, że dane szkoleniowe są często wątpliwej jakości i nie są neutralne;

C. mając na uwadze, że postęp technologii komunikacyjnych oraz wszechobecnie stosowane urządzenia elektroniczne, przyrządy monitorujące, media społecznościowe, powiązania z internetem i sieci internetowe, w tym urządzenia przekazujące informacje bez udziału człowieka, doprowadziły do rozwinięcia masy stale rosnących zbiorów danych, które poprzez zaawansowane techniki przetwarzania i analizy umożliwiają niespotykany do tej pory wgląd w zachowanie ludzi, życie prywatne i życie naszych społeczeństw;

D. mając na uwadze, że służby wywiadowcze państw trzecich i państw członkowskich w coraz większym stopniu polegają na przetwarzaniu i analizie takich zbiorów danych, które nie podlegają żadnym ramom prawnym lub w ostatnim czasie stały się przedmiotem przepisów prawnych, których zgodność z unijnym prawem pierwotnym i wtórnym budzi wątpliwości i wymaga potwierdzenia;

E. mając na uwadze, że nasilenie zjawisk takich jak nękanie, przemoc wobec kobiet i podatność dzieci na zagrożenia ma miejsce również w środowisku internetowym; mając na uwadze, że Komisja i państwa członkowskie powinny przyjąć wszelkie niezbędne środki prawne w celu przeciwdziałania tym zjawiskom;

F. mając na uwadze, że coraz więcej korporacji, przedsiębiorstw, organów, agencji, organizacji rządowych i pozarządowych (jak i ogólnie sektor publiczny i prywatny), przywódców politycznych, podmiotów społeczeństwa obywatelskiego, środowisk akademickich i naukowych oraz obywateli wykorzystuje takie zbiory danych i korzysta z analizy dużych zbiorów danych dla celów związanych z konkurencyjnością, innowacyjnością, prognozowaniem rynkowym, kampaniami politycznymi, ukierunkowaną reklamą, badaniami naukowymi i kształtowaniem polityki w dziedzinie transportu, opodatkowania, usług finansowych, inteligentnych miast, egzekwowania prawa, przejrzystości, zdrowia publicznego i reagowania na klęski naturalne, a także w celu wpływania na wyniki wyborcze i polityczne na przykład poprzez ukierunkowaną komunikację;

G. mając na uwadze, że rynek dużych zbiorów danych rośnie, w miarę jak coraz powszechniej akceptuje się technologie i procesy podejmowania decyzji w oparciu o dane, uznając, że zapewniają one rozwiązania; mając na uwadze, że nie opracowano jeszcze metodologii potrzebnej do przeprowadzenia opartej na faktach oceny całkowitego wpływu dużych zbiorów danych, istnieją jednak dowody wskazujące na to, że analiza dużych zbiorów danych może mieć istotne oddziaływanie horyzontalne zarówno w sektorze publicznym, jak i prywatnym; mając na uwadze, że w przedstawionej przez Komisję strategii jednolitego rynku cyfrowego dla Europy uznano potencjał opartych na danych technologii, usług i dużych zbiorów danych jako czynnika wspomagającego wzrost gospodarczy, innowacje i cyfryzację w UE;

H. mając na uwadze, że analiza dużych zbiorów danych na różne sposoby generuje wartość dodaną, na co wskazują liczne pozytywne przykłady wiążące się z istotnymi korzyściami dla obywateli, np. w dziedzinie opieki zdrowotnej, walki ze zmianą klimatu, obniżania zużycia energii, poprawy bezpieczeństwa w transporcie i rozwoju inteligentnych miast, przez co optymalizuje się działalność przedsiębiorstw i podnosi ich skuteczność, a także poprawia warunki pracy oraz

([1]) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

wykrywa i zwalcza nadużycia; mając na uwadze, że technologia dużych zbiorów danych może być źródłem przewagi konkurencyjnej w procesach podejmowania decyzji w europejskich przedsiębiorstwach, a sektor publiczny może czerpać korzyści z większej skuteczności dzięki lepszemu zrozumieniu rozwoju społeczno-gospodarczego na jego różnych poziomach;

I. mając na uwadze, że duże zbiory danych charakteryzują się wspomnianymi wyżej korzyściami dla obywateli, środowisk akademickich i naukowych oraz sektora publicznego i prywatnego, ale wiążą się również z poważnymi zagrożeniami, mianowicie w zakresie ochrony praw podstawowych, takich jak prawo do ochrony prywatności i danych osobowych oraz prawo do bezpieczeństwa danych, ale także wolności słowa i niedyskryminacji, gwarantowanych Kartą praw podstawowych Unii Europejskiej i prawodawstwem unijnym; mając na uwadze, że techniki pseudonimizacji i szyfrowania mogą ograniczać ryzyko związane z analizą dużych zbiorów danych i dlatego odgrywają ważną rolę w ochronie prywatności podmiotu danych, a jednocześnie pozytywnie wpływają na innowacje i wzrost gospodarczy; mając na uwadze, że elementy te należy postrzegać jako objęte obecnym przeglądem dyrektywy o prywatności i łączności elektronicznej;

J. mając na uwadze, że wszechobecność czujników, szerokie rutynowe wytwarzanie danych i współczesne czynności przetwarzania danych nie zawsze są wystarczająco przejrzyste, co ogranicza zdolność obywateli i władz do oceny procesów oraz celu gromadzenia, kompilacji, analizy i sposobu wykorzystania danych osobowych; mając na uwadze, że zacieranie się granic między danymi osobowymi a danymi nieosobowymi może wynikać ze stosowania analizy dużych zbiorów danych, co może prowadzić do tworzenia nowych danych osobowych;

K. mając na uwadze, że sektor dużych zbiorów danych rośnie o 40 % rocznie, czyli siedmiokrotnie szybciej niż rynek informatyczny; mając na uwadze, że koncentracja dużych zbiorów danych wytwarzanych wskutek nowych technologii oferuje informacje o kluczowym znaczeniu dla dużych korporacji, co pociąga za sobą bezprecedensowe zmiany w równowadze sił między obywatelami, rządami i podmiotami prywatnymi; mając na uwadze, że taka koncentracja siły w rękach korporacji może utwierdzać monopole i praktyki stanowiące nadużycie oraz negatywnie wpływać na prawa konsumentów i uczciwą konkurencję rynkową; mając na uwadze, że interesy jednostki oraz ochrona praw podstawowych wymagają dokładniejszej kontroli w kontekście łączenia dużych zbiorów danych;

L. mając na uwadze, że duże zbiory danych mają ogromny, niezrealizowany potencjał jako czynnik wspomagający produktywność i jako sposób na oferowanie obywatelom lepszych produktów i usług; podkreśla jednak, że powszechne korzystanie z inteligentnych urządzeń, sieci i aplikacji internetowych przez obywateli, przedsiębiorstwa i organizacje nie musi oznaczać zadowolenia z oferowanych produktów, lecz raczej wskazuje na szersze zrozumienie, że usługi te stały się niezbędne do życia, komunikacji i pracy pomimo braku zrozumienia zagrożeń, jakie mogą one stwarzać dla naszego dobrego samopoczucia, bezpieczeństwa i dla naszych praw;

M. mając na uwadze, że konieczne jest rozróżnienie między ilością a jakością danych, aby ułatwić skuteczne wykorzystanie dużych zbiorów danych (za pomocą algorytmów i innych narzędzi analitycznych); mając na uwadze, że niskiej jakości dane lub niskiej jakości procedury będące podstawą procesów decyzyjnych i narzędzi analitycznych mogą skutkować nieobiektywnymi algorytmami, fałszywymi korelacjami, błędami, niedocenianiem skutków prawnych, społecznych i etycznych, możliwością wykorzystania danych do celów dyskryminacyjnych lub do nadużyć oraz marginalizacją roli człowieka w tych procesach, co może prowadzić do błędnych procedur podejmowania decyzji negatywnie oddziałujących na życie i możliwości obywateli, zwłaszcza grup zmarginalizowanych, a także mieć negatywny wpływ na społeczeństwa i przedsiębiorstwa;

N. mając na uwadze, że rozliczalność za stosowanie algorytmów i przejrzystość powinny oznaczać wdrażanie środków technicznych i operacyjnych gwarantujących przejrzystość, niedyskryminację zautomatyzowanego procesu podejmowania decyzji i obliczanie prawdopodobieństwa indywidualnego zachowania; mając na uwadze, że przejrzystość powinna umożliwiać jednostkom otrzymywanie istotnych informacji o rządzących zasadach, znaczeniu i przewidywanych konsekwencjach; mając na uwadze, że powinno to obejmować informacje o danych wykorzystywanych na potrzeby szkoleń w zakresie analizy dużych zbiorów danych oraz umożliwiać jednostkom zrozumienie i monitorowanie decyzji mających na nie wpływ;

O. mając na uwadze, że analiza danych i algorytmy w coraz większym stopniu wpływają na informacje udostępniane obywatelom; mając na uwadze, że techniki te w razie niewłaściwego stosowania mogą zagrozić poszanowaniu praw podstawowych do informacji oraz wolności i pluralizmowi mediów; mając na uwadze, że system nadawania publicznego w państwach członkowskich jest bezpośrednio związany z potrzebami demokratycznymi, społecznymi i kulturowymi każdego społeczeństwa oraz z potrzebą zachowania pluralizmu mediów, jak określono w protokole w sprawie systemu publicznego nadawania w państwach członkowskich, dołączonym do traktatu z Amsterdamu (11997D/PRO/09);

P. mając na uwadze, że mnożenie się przetwarzania i analizowania danych, multum podmiotów uczestniczących w gromadzeniu, zatrzymywaniu, przetwarzaniu, przechowywaniu i wymianie danych, a także łączenie dużych zbiorów danych zawierających dane osobowe i nieosobowe z przeróżnych źródeł oznacza co prawda znaczne możliwości, ale wywołało także ogromną niepewność wśród obywateli oraz w sektorze publicznym i prywatnym co do specjalnych wymogów dotyczących zgodności z obowiązującymi w UE zasadami ochrony danych;

Q. mając na uwadze, że istnieje nadmiar nieustrukturyzowanych przestarzałych systemów zawierających duże ilości danych zgromadzonych przez lata przez przedsiębiorstwa, objętych niejasnymi systemami zarządzania danymi, które należy systematycznie dostosowywać do obowiązujących przepisów;

R. mając na uwadze, że należy dążyć do zacieśniania współpracy i do większej spójności między różnymi organami regulacyjnymi oraz organami ds. nadzoru nad konkurencją, organami ds. ochrony konsumentów i organami ochrony danych na szczeblu krajowym i unijnym, aby zagwarantować spójne podejście w odniesieniu do konsekwencji wynikających dla praw podstawowych ze stosowania dużych zbiorów danych oraz zrozumienie tychże konsekwencji; mając na uwadze, że ustanowienie i dalszy rozwój cyfrowej izby rozliczeniowej ([1]) jako opartej na zasadzie dobrowolności sieci organów ścigania może przyczynić się do usprawnienia ich pracy i prowadzonych przez nie czynności z zakresu egzekwowania przepisów, a także może pogłębić efekty synergii oraz skutkować lepszą ochroną praw i interesów jednostek;

Uwagi ogólne

1. podkreśla, że obywatele, sektor publiczny i prywatny oraz środowiska akademickie i naukowe będą mogły w pełni wykorzystać perspektywy i możliwości, jakie niosą ze sobą duże zbiory danych, kiedy zostanie zapewnione publiczne zaufanie do tych technologii dzięki ścisłemu przestrzeganiu praw podstawowych i obowiązujących w UE przepisów w zakresie ochrony danych, a także dzięki pewności prawnej dla wszystkich zainteresowanych podmiotów; podkreśla, że przetwarzanie danych osobowych możliwe jest jedynie w oparciu o podstawy prawne określone w art. 6 rozporządzenia (UE) 2016/679; uważa, że przejrzystość i należyte informowanie zainteresowanych grup docelowych ma kluczowe znaczenie dla budowania zaufania publicznego oraz dla ochrony praw indywidualnych;

2. podkreśla, że przestrzeganie istniejących przepisów prawnych w zakresie ochrony danych oraz wysokie standardy naukowe i etyczne to elementy o kluczowym znaczeniu dla budowania zaufania do rozwiązań, których podstawą są duże zbiory danych, oraz dla niezawodności tych rozwiązań; podkreśla ponadto, że informacje ujawniane w wyniku analizy dużych zbiorów danych nie przedstawiają żadnej kwestii w sposób bezstronny i są wiarygodne jedynie na tyle, na ile umożliwiają to dane bazowe; podkreśla, że badania prognostyczne oparte na dużych zbiorach danych mogą zaoferować jedynie prawdopodobieństwo statystyczne i wobec tego nie zawsze mogą służyć do dokładnego przewidywania indywidualnych zachowań; w związku z tym podkreśla, że potrzebne są solidne standardy naukowe i etyczne, aby zarządzać gromadzeniem danych i oceniać wyniki takich analiz;

3. zaznacza, że szczególnie chronione informacje o osobach można wywnioskować z danych niewymagających ochrony, co prowadzi do zatarcia różnicy między jednym a drugim rodzajem danych;

4. podkreśla, że niski poziom wiedzy i zrozumienia wśród obywateli na temat charakteru dużych zbiorów danych umożliwia wykorzystywanie danych osobowych w sposób inny niż zamierzony; zauważa, że w UE niezwykle ważna jest edukacja i działalność uświadamiająca w kwestii praw podstawowych; wzywa instytucje UE i państwa członkowskie do inwestowania w umiejętności cyfrowe i działania uświadamiające w zakresie praw cyfrowych, prywatności i ochrony danych wśród obywateli, w tym również wśród dzieci; podkreśla, że tego typu edukacja powinna uwzględniać zrozumienie zasad i logiki działania algorytmów i procesów automatycznego podejmowania decyzji oraz tego, jak merytorycznie je interpretować; ponadto podkreśla potrzebę edukacji wspomagającej zrozumienie, gdzie i jak gromadzone są strumienie

([1]) Opinia Europejskiego Inspektora Ochrony Danych nr 8/2016 z dnia 23 września 2016 r., s. 15.

danych (pozyskiwanie danych z internetu, łączenie danych przesyłanych strumieniowo z danymi z sieci społecznościowych i urządzeń połączonych oraz ich agregowanie w nowy strumień danych);

Duże zbiory danych do celów handlowych i w sektorze publicznym

Ochrona prywatności i danych

5. wskazuje, że unijne przepisy w zakresie ochrony prywatności i danych osobowych, prawo do równości, zasada niedyskryminacji, przysługujące jednostkom prawo do otrzymywania informacji na temat zasad automatycznego podejmowania decyzji i profilowania oraz prawo do dochodzenia roszczeń mają zastosowanie w przetwarzaniu danych, gdy przetwarzanie jest poprzedzone technikami pseudonimizacji, a także w każdym przypadku, kiedy wykorzystanie danych nieosobowych może mieć wpływ na prywatne życie osób lub inne prawa i wolności oraz prowadzić do stygmatyzacji całych grup społecznych;

6. podkreśla, że jednolity rynek cyfrowy należy zbudować w oparciu o niezawodne, godne zaufania i bardzo szybkie sieci i usługi, które chronią prawa podstawowe osób, których dane dotyczą, do ochrony danych osobowych i prywatności przy jednoczesnym zachęcaniu do innowacji i analizy dużych zbiorów danych, aby stworzyć właściwe warunki działania i zagwarantować równe szanse z myślą o wspomożeniu europejskiej gospodarki cyfrowej;

7. ponadto podkreśla możliwość ponownej identyfikacji jednostek poprzez skorelowanie różnych rodzajów zanonimizowanych danych; podkreśla, że prawo Unii w zakresie ochrony prywatności i danych osobowych ma zastosowanie do przetwarzania takich skorelowanych danych tylko wówczas, gdy rzeczywiście istnieje możliwość ponownej identyfikacji jednostki;

8. podkreśla, że wspomniane wyżej zasady powinny służyć jako ramy na potrzeby procedur podejmowania decyzji w sektorze publicznym i prywatnym oraz przez inne podmioty wykorzystujące dane; podkreśla potrzebę dużo większego nacisku na rozliczalność za stosowanie algorytmów oraz przejrzystość w odniesieniu do przetwarzania i analizowania danych przez sektor publiczny i prywatny oraz wszelkie inne podmioty korzystające z analizy danych, gdyż są to podstawowe narzędzia gwarantujące, że jednostka będzie należycie poinformowana o przetwarzaniu jej danych osobowych;

9. podkreśla fundamentalną rolę, jaką Komisja, Europejska Rada Ochrony Danych, krajowe organy ochrony danych osobowych i inne niezależne organy nadzorcze powinny w przyszłości odgrywać, aby promować przejrzystość, sprawiedliwość proceduralną oraz pewność prawa dotyczącego ogólnych i konkretnych standardów ochrony praw podstawowych i gwarancji związanych z wykorzystywaniem przetwarzania i analizowanych danych w sektorze publicznym i prywatnym; apeluje o ściślejszą współpracę między organami regulującymi zachowania w środowisku cyfrowym, aby w ten sposób wzmocnić efekty synergii między ramami regulacyjnymi dla konsumentów a organami ds. ochrony konkurencji i danych osobowych; wzywa do wyposażenia tych organów w odpowiednie środki finansowe i kadrowe; dostrzega ponadto potrzebę powołania cyfrowej izby rozliczeniowej;

10. podkreśla, że istotą dużych zbiorów danych powinno być osiąganie porównywalnych korelacji przy użyciu jak najmniejszej liczby danych osobowych; podkreśla w związku z tym, że środowiska naukowe, biznesowe i publiczne powinny skupić się na badaniach i innowacjach w dziedzinie anonimizacji;

11. przyznaje, że stosowanie pseudonimizacji, anonimizacji lub szyfrowania danych osobowych może zmniejszać ryzyko dla osób, których dane dotyczą, kiedy dane osobowe wykorzystuje się w zastosowaniach opartych na dużych zbiorach danych; zwraca ponadto uwagę na korzyści płynące z pseudonimizacji, o której mowa w ogólnym rozporządzeniu o ochronie danych, stanowiącej właściwe zabezpieczenie; przypomina, że anonimizacja stanowi nieodwracalny proces, w wyniku którego nie można już wykorzystywać danych osobowych jedynie w celu identyfikacji lub wskazania konkretnej osoby fizycznej; jest zdania, że zobowiązania umowne powinny gwarantować, że zanonimizowane dane nie będą mogły zostać ponownie przyporządkowane przy użyciu dodatkowych korelacji w drodze łączenia różnych źródeł danych; apeluje do sektora publicznego i prywatnego, a także do innych podmiotów zaangażowanych w analizę dużych zbiorów danych o regularne przeprowadzanie przeglądu takich zagrożeń w świetle nowych technologii oraz o dokumentowanie trafności przyjętych środków; apeluje do Komisji, Europejskiej Rady Ochrony Danych i innych niezależnych organów nadzorczych o przygotowanie wytycznych dotyczących prawidłowego

anonimizowania danych, aby uniknąć w przyszłości nadużyć w stosowaniu tych środków oraz monitorować stosowane praktyki;

12. wzywa sektor prywatny i publiczny oraz innych administratorów danych do korzystania z instrumentów przewidzianych w ogólnym rozporządzeniu o ochronie danych, takich jak kodeksy postępowania i systemy certyfikacji, aby dążyć do większej pewności w zakresie konkretnych obowiązków, jakie nakłada na nie prawo unijne, oraz do zapewnienia zgodności stosowanych przez nie praktyk i prowadzonych działań z odpowiednimi unijnymi standardami i gwarancjami prawnymi;

13. wzywa Komisję i państwa członkowskie do zadbania o to, by technologie oparte na danych nie zawężały ani nie ograniczały w dyskryminacyjny sposób dostępu do pluralistycznego środowiska medialnego, lecz wspierały wolność i pluralizm mediów; podkreśla, że współpraca między rządami, instytucjami kształcenia i organizacjami medialnymi będzie odgrywać centralną rolę w dążeniu do tego, by wspierano umiejętność korzystania z mediów cyfrowych z myślą o wzmocnieniu pozycji obywateli oraz ochronie ich prawa do informacji i wolności wypowiedzi;

14. jest zdania, że publikację danych osobowych przez organy publiczne z przyczyn związanych z interesem publicznym, takich jak zapobieganie korupcji, konfliktom interesów, oszustwom podatkowym i praniu pieniędzy, można dopuścić w demokratycznym społeczeństwie, pod warunkiem że dane ujawnia się na warunkach określonych przepisami prawa i wprowadzono odpowiednie zabezpieczenia, a publikacja taka jest niezbędna w danym celu i proporcjonalna;

Bezpieczeństwo

15. uznaje wartość dodaną rozwoju technologicznego, który przyczyni się do poprawy bezpieczeństwa; przyznaje, że niektóre z najbardziej palących zagrożeń związanych z czynnościami przetwarzania danych, takimi jak techniki dotyczące dużych zbiorów danych (zwłaszcza w kontekście internetu rzeczy), budzących niepokój obywateli, to naruszenie bezpieczeństwa, niedozwolony dostęp do danych i nielegalna inwigilacja; uważa, że uporanie się z takimi zagrożeniami bez naruszenia praw podstawowych wymaga prawdziwej i skoordynowanej współpracy między sektorem prywatnym i publicznym, organami egzekwowania prawa i niezależnymi organami nadzorczymi; w związku z tym podkreśla, że szczególną uwagę należy zwrócić na bezpieczeństwo systemów administracji elektronicznej, a także na dodatkowe środki prawne, takie jak odpowiedzialność za oprogramowanie;

16. jest zdania, że należy też zachęcać do stosowania pełnego szyfrowania transmisji, a w razie konieczności je nakazywać, zgodnie z zasadą uwzględnienia ochrony danych już w fazie projektowania; zaleca w tym względzie, aby wszelkie przyszłe ramy ustawodawcze wyraźnie zabraniały dostawcom usług szyfrowania, usług komunikacyjnych i innym organizacjom (na wszystkich poziomach łańcucha dostaw), by ci umożliwiali lub ułatwiali stosowanie celowo pozostawionych luk w zabezpieczeniach;

17. podkreśla, że intensywne generowanie danych i wzmożone przepływy danych wiążą się z nowymi zagrożeniami oraz nowymi wyzwaniami w dziedzinie bezpieczeństwa informacji; w związku z tym apeluje o uwzględnianie ochrony prywatności już w fazie projektowania oraz o domyślną ochronę prywatności, stosowanie w odpowiednich przypadkach technik anonimizacji i technik szyfrowania oraz o przeprowadzanie obowiązkowej oceny skutków w zakresie ochrony prywatności; podkreśla, że środki takie powinny być stosowane przez wszystkie podmioty zaangażowane w analizę dużych zbiorów danych w sektorze prywatnym i publicznym, a także inne podmioty mające do czynienia z danymi wymagającymi szczególnej ochrony, takie jak prawnicy, dziennikarze i pracownicy służby zdrowia, aby korzystanie z dużych zbiorów danych nie skutkowało zwiększeniem podatności na zagrożenia związane z bezpieczeństwem informacji;

18. przypomina, że zgodnie z art. 15 dyrektywy 2000/31/WE państwa członkowskie nie mogą nakładać na usługodawców świadczących usługi transmisji, przechowywania i hostingu ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują, ani ogólnego obowiązku aktywnego poszukiwania faktów lub okoliczności wskazujących na bezprawną działalność; przypomina w szczególności, że Trybunał Sprawiedliwości Unii Europejskiej w sprawach C-360/10 i C-70/10 odrzucił środki „aktywnego nadzoru" nad prawie wszystkimi usługobiorcami (w jednej sprawie chodziło o dostawców usług internetowych, a w drugiej – o sieć społecznościową) i sprecyzował, że wszelkie narzucanie podmiotom świadczącym usługi hostingu obowiązku prowadzenia ogólnego nadzoru jest zakazane;

Niedyskryminacja

19. podkreśla, że z powodu korzystania ze zbiorów danych i systemów algorytmicznych w ramach przeprowadzania ocen i sporządzania prognoz na różnych etapach przetwarzania danych technologia dużych zbiorów danych może prowadzić nie tylko do naruszania podstawowych praw jednostek, ale również skutkować zróżnicowanym traktowaniem i pośrednią dyskryminacją grup społecznych o podobnej charakterystyce, zwłaszcza w kwestii uczciwych i równych szans

dostępu do edukacji i zatrudnienia, podczas naboru lub oceny jednostek, albo też w kontekście określania nowych przyzwyczajeń użytkowników mediów społecznościowych w związku z ich rolą jako konsumentów;

20. wzywa Komisję, państwa członkowskie i organy ochrony danych do określenia i podjęcia wszelkich możliwych środków służących ograniczeniu do minimum algorytmicznej dyskryminacji i uprzedzeń oraz do opracowania solidnych i wspólnych ram etycznych na potrzeby przejrzystego przetwarzania danych osobowych i automatycznego podejmowania decyzji, tak aby ramy te mogły być pomocą w korzystaniu z danych i bieżącym egzekwowaniu prawa Unii;

21. wzywa Komisję, państwa członkowskie i organy ochrony danych do przeprowadzenia konkretnej oceny konieczności zapewnienia nie tylko przejrzystości algorytmów, lecz także przejrzystości w odniesieniu do możliwych uprzedzeń w danych szkoleniowych wykorzystywanych do wyciągania wniosków na podstawie dużych zbiorów danych;

22. zaleca, aby przedsiębiorstwa regularnie przeprowadzały oceny reprezentatywności swoich zbiorów danych, sprawdzały, czy nie pojawiają się w nich elementy uprzedzenia, i opracowywały strategie przezwyciężania tych uprzedzeń; podkreśla potrzebę analizowania precyzyjności i znaczenia prognoz opartych na analizie danych pod kątem sprawiedliwości i zasad etycznych;

Duże zbiory danych do celów naukowych

23. podkreśla, że analiza dużych zbiorów danych może być korzystna dla rozwoju nauki i badań naukowych; uważa, że rozwój analizy dużych zbiorów danych i korzystanie z niej w celach naukowych musi odbywać się z należytym poszanowaniem podstawowych wartości określonych w Karcie praw podstawowych Unii Europejskiej i zgodnie z aktualnym prawodawstwem unijnym w zakresie ochrony danych;

24. przypomina, że na mocy ogólnego rozporządzenia o ochronie danych dalsze przetwarzanie danych osobowych w celach statystycznych może prowadzić jedynie do powstania danych zagregowanych, z których nie można ponownie wywnioskować danych odnoszących się do jednostek;

Duże zbiory danych do celów egzekwowania prawa

Ochrona prywatności i danych

25. przypomina wszystkim podmiotom zajmującym się egzekwowaniem prawa, które stosują przetwarzanie i analizę danych, że w dyrektywie (UE) 2016/680: uregulowano przetwarzanie danych osobowych przez państwa członkowskie do celów egzekwowania prawa; zawarto wymóg, zgodnie z którym gromadzenie i przetwarzanie danych osobowych do celów egzekwowania prawa zawsze musi być odpowiednie i rzeczowe oraz nie może wykraczać poza konkretne, wyraźne i prawnie uzasadnione cele, w związku z którymi dane są przetwarzane; stwierdzono, iż jednoznacznie należy wskazać cel i potrzebę gromadzenia tych danych; postanowiono, iż decyzje opierające się wyłącznie na zautomatyzowanym przetwarzaniu, w tym również na profilowaniu, i mające niekorzystne skutki prawne dla podmiotu danych lub poważnie nań wpływające są zakazane, chyba że dopuszcza je prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator i które przewiduje odpowiednie zabezpieczenia praw i wolności podmiotu danych, a przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora; wzywa Komisję, Europejską Radę Ochrony Danych i inne niezależne organy nadzorcze o opublikowanie wytycznych, zaleceń i najlepszych praktyk, aby doprecyzować kryteria i warunki dotyczące decyzji, których podstawą jest profilowanie oraz korzystanie z dużych zbiorów danych do celów egzekwowania prawa;

26. podkreśla znaczenie, jakie ma zapewnienie zgodności z dyrektywą (UE) 2016/680 w odniesieniu do przeprowadzania uprzednich ocen wpływu i kontroli uwzględniających obawy etyczne, aby ocenić inkluzywny charakter, dokładność i jakość danych oraz zadbać o to, aby osoby, których dotyczą decyzje, lub podmioty uczestniczące w procesie decyzyjnym były w stanie zrozumieć i zakwestionować gromadzenie lub analizę danych, wzorce i korelacje oraz zapobiec szkodliwym konsekwencjom dla niektórych grup ludzi;

27. zaznacza, że działania rządów i organów egzekwowania prawa polegające na masowej inwigilacji i nieuzasadnionym dostępie do danych handlowych i innych danych osobowych mogą poważnie podważyć zaufanie obywateli do usług cyfrowych;

28. przypomina, że prawodawstwo zezwalające organom publicznym na regularny dostęp do treści komunikacji elektronicznej należy uznać za narażające na szwank istotę podstawowego prawa do poszanowania życia prywatnego, zagwarantowanego na mocy art. 7 Karty praw podstawowych Unii Europejskiej;

29. podkreśla potrzebę włączenia wytycznych i systemów do zasad udzielania zamówień publicznych na modele, narzędzia i programy przetwarzania danych w oparciu o duże zbiory danych, przeznaczone do celów egzekwowania prawa, aby zagwarantować, że przed dokonaniem ostatecznego zakupu organ egzekwowania prawa może sprawdzić i sprawdza kod źródłowy tych modeli, narzędzi i programów pod kątem jego zgodności, poprawności i bezpieczeństwa, przy czym należy brać pod uwagę, że oprogramowanie zamknięte ogranicza przejrzystość i rozliczalność; zaznacza, że pewne modele prowadzenia prewencyjnych działań policyjnych bardziej sprzyjają prywatności niż inne, np. jeśli prognozy probabilistyczne dotyczą miejsc lub zdarzeń, a nie pojedynczych osób;

Bezpieczeństwo

30. podkreśla bezwzględną potrzebę ochrony baz danych organów ścigania przed naruszeniem zasad bezpieczeństwa i bezprawnym dostępem, gdyż jest to przedmiotem obaw obywateli; uważa wobec tego, że uporanie się z takimi zagrożeniami wymaga skoordynowanej i skutecznej współpracy między organami egzekwowania prawa, sektorem prywatnym, rządami i niezależnymi organami nadzorującymi ochronę danych; żąda gwarancji odpowiednich zabezpieczeń danych osobowych zgodnie z rozporządzeniem (UE) 2016/679 i dyrektywą (UE) 2016/680, a także minimalizacji zagrożeń za pomocą bezpiecznej i zdecentralizowanej architektury baz danych;

Niedyskryminacja

31. ostrzega, że ze względu na intruzywny charakter decyzji i środków podejmowanych przez organy egzekwowania prawa, w tym również w oparciu o przetwarzanie i analizę danych, odnośnie do życia i praw obywateli potrzebna jest maksymalna ostrożność, aby uniknąć nielegalnej dyskryminacji i obierania za cel danej osoby lub grupy osób, wyodrębnionych ze względu na rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, majątek, urodzenie, niepełnosprawność, wiek, płeć, ekspresję płciową, tożsamość płciową, orientację seksualną, status pobytowy, stan zdrowia lub przynależność do mniejszości narodowej, co często jest przedmiotem profilowania etnicznego lub intensywniejszych działań nadzorczych w zakresie egzekwowania prawa, a także jednostek posiadających cechy szczególne; wzywa do właściwego szkolenia osób bezpośrednio odpowiedzialnych za gromadzenie danych i użytkowników informacji uzyskiwanych w wyniku analizy danych;

32. wzywa organy egzekwowania prawa państw członkowskich, które wykorzystują analizę danych, do przestrzegania najwyższych standardów etycznych podczas analizowania danych i do zapewnienia udziału ludzi oraz rozliczalności na poszczególnych etapach podejmowania decyzji, nie tylko aby ocenić reprezentatywność, dokładność i jakość danych, lecz także aby ocenić trafność każdej decyzji podejmowanej na podstawie takich informacji;

o

o o

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