Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Tożsamość cyfrowa, suwerenność danych i droga do sprawiedliwej transformacji cyfrowej dla obywateli żyjących w społeczeństwie informacyjnym”

(opinia z inicjatywy własnej)

(2022/C 443/03)

Sprawozdawca: **Dumitru FORNEA**

Podstawa prawna	Art. 52 ust. 2 regulaminu wewnętrznego
	Opinia z inicjatywy własnej
Decyzja Zgromadzenia Plenarnego	20.1.2022
Sekcja odpowiedzialna	Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego
Data przyjęcia przez sekcję	21.6.2022
Data przyjęcia na sesji plenarnej	14.7./2022
Sesja plenarna nr	571
Wynik głosowania	
(za/przeciw/wstrzymało się)	179/1/3

1. **Wnioski i zalecenia**

1.1. Postęp technologiczny i ewolucja technologii cyfrowych, biotechnologii i systemów łączności elektronicznej stworzyły istotne możliwości konsolidacji zamożnych, bardziej integracyjnych i sprawiedliwych społeczeństw. Jednocześnie wzrosła liczba zagrożeń dla ludzkości.

1.2. Aby zachować bezpieczeństwo ludzkości i tkankę społeczną niezbędną do tego, aby każda osoba na naszej planecie mogła wieść satysfakcjonujące życie, musimy zadbać o to, by nowe narzędzia zarządzania narzucone przez rewolucję cyfrową i przemysłową nie były uciążliwe i nie uzależniały codziennego życia od obowiązku przynależności do cyfrowych systemów technologicznych kontrolowanych w niedemokratyczny sposób.

1.3. Instytucje publiczne są narażone na ataki ze strony podmiotów niepaństwowych mających bezpośredni dostęp do wiedzy, patentów, technologii i funduszy inwestycyjnych. **Europejski Komitet Ekonomiczno-Społeczny (**EKES) uważa, że we wszystkich przyszłych działaniach politycznych należy uwzględnić europejską suwerenność technologiczną oraz że należy uzupełnić prawodawstwo o przejrzyste i mające pełne zastosowanie przepisy i wspólne normy we wszystkich państwach członkowskich.

1.4. Rozwój technologiczny oddziałuje na wiele praw i wolności obywateli. Komitet postuluje, aby wszystkie sektory wykorzystujące dane osobowe i biometryczne regulować w jasny sposób i w pełnej zgodności z podstawowymi prawami człowieka, oraz wzywa do odpowiedniej aktualizacji ogólnego rozporządzenia o ochronie danych (RODO).

1.5. EKES jest przekonany, że tożsamość cyfrowa, cyfrowe środki płatnicze oraz włączenie do platform rzeczywistości wirtualnej i rozszerzonej powinny pozostać narzędziami, które jedynie uzupełniają fizyczne istnienie, jakie znaliśmy przed pojawieniem się tych technologii. Nie powinny całkowicie ani nadmiernie wypierać innych wzorców egzystencji, które były rozwijane i doskonalone przez ludzi na przestrzeni tysięcy lat ich istnienia.

1.6. EKES wzywa do zawarcia jasnych przepisów antydyskryminacyjnych we wszystkich przyszłych wnioskach ustawodawczych dotyczących tożsamości cyfrowej i całkowicie sprzeciwia się wprowadzeniu systemu, który umożliwia dokładną obserwację obywateli Unii, ich śledzenie lub monitorowanie ich działań i zachowań. Ponadto Komitet uważa za konieczne, aby zorganizowane społeczeństwo obywatelskie było w pełni zaangażowane w proces wdrażania.

1.7. EKES doszedł do wniosku, że wszelkie inicjatywy służące włączeniu obywateli do europejskiego systemu tożsamości cyfrowej powinny opierać się na badaniach wpływu i kompleksowych badaniach socjologicznych. Ostateczną decyzję należy podjąć wyłącznie za świadomą i dobrowolnie wyrażoną zgodą obywatela.

1.8. Komitet uważa, że aby demokratycznie dążyć do stworzenia sprawiedliwego, akceptowanego przez obywateli UE społeczeństwa cyfrowego, Komisja musi przeprowadzić oceny skutków dotyczące:

— ogromnego i całodobowego zapotrzebowania na energię niezbędną do utrzymania globalnej infrastruktury technologicznej zapewniającej nieprzerwany i bezpieczny dostęp do systemu cyfrowego, którego celem jest przekazywanie najważniejszych i strategicznych funkcji społeczeństwa,

— wpływu cyfryzacji i automatyzacji interakcji międzyludzkich na jakość życia i warunki pracy (zwłaszcza na relacje międzyludzkie), wzrostu częstości występowania samotności, problemów ze zdrowiem psychicznym, spadku inteligencji poznawczej i emocjonalnej oraz zwiększonego ryzyka alienacji społecznej,

— środków politycznych, gospodarczych i społecznych niezbędnych do przystosowania społeczeństwa do radykalnych zmian ilościowych na rynku pracy,

— cyberbezpieczeństwa, w kontekście zwiększonej różnorodności i złożoności działań hakerów oraz w warunkach przyspieszonego tempa rozwoju internetu rzeczy, co sprawia, że protokoły dostępu są podatne na ataki i nieefektywne.

1.9. EKES stwierdza, że bezpieczeństwo danych nie powinno podlegać negocjacjom, i jest rozczarowany, że bezpieczeństwo przyszłego europejskiego portfela cyfrowego nie jest głównym priorytetem wniosku ustawodawczego Komisji.

1.10. Komitet uważa, że we wszystkich wnioskach ustawodawczych UE dotyczących sztucznej inteligencji należy wyraźnie przewidzieć pełną rozliczalność za ewentualne nieprawidłowe działanie. Należy znaleźć odpowiednią równowagę między nieujawnianiem tajemnic handlowych a zapewnieniem przejrzystości i możliwości śledzenia rozwoju sytuacji.

1.11. Komitet jest pierwszą instytucją europejską, która zaleciła przyjęcie podejścia opartego na ludzkiej kontroli, i ponownie podkreśla potrzebę istnienia kilku poziomów kontroli, aby ją zapewnić.

1.12. EKES jest całkowicie przeciwny prywatnym bazom danych służącym rozpoznawaniu twarzy (z wyjątkiem zastosowań związanych z przestępczością) oraz wszelkim rodzajom systemów scoringu obywateli, ponieważ naruszają one podstawowe wartości i prawa UE.

1.13. Komitet uważa, że dane pochodzące z UE powinny być przechowywane na terytorium UE i powinny być chronione przed jakimkolwiek dostępem z zewnątrz. Ponadto EKES uważa, że w odniesieniu zarówno do danych osobowych, jak i nieosobowych należy wprowadzać świadomą zgodę na wykorzystanie danych, i ponownie wzywa do ulepszenia RODO w tym zakresie.

1.14. Komitet wyraża zaniepokojenie rosnącymi nierównościami między państwami członkowskimi oraz brakiem ochrony słabszych grup i jeszcze raz wzywa do tworzenia UE, która popiera włączenie cyfrowe niepozostawiające nikogo w tyle. Szczególną uwagę należy zwrócić na starsze pokolenie.

1.15. EKES wzywa do tworzenia silnego europejskiego systemu edukacji cyfrowej, który może przygotować siłę roboczą do wyzwań technologicznych i pomóc jej w zdobyciu miejsc pracy wysokiej jakości. We wszystkich państwach członkowskich należy wdrożyć programy rozwoju umiejętności cyfrowych, a także programy cyfrowego uczenia się przez całe życie, kursy słownictwa i praktyczne szkolenia.

1.16. Komitet uważa, że zaangażowanie pracowników w proces transformacji cyfrowej jest niezbędne, aby mogli oni zrozumieć związane z nią przyszłe zagrożenia i możliwości. Umożliwi to transfer wiedzy i zdobywanie nowych umiejętności.

2. **Kontekst**

2.1. Obywatelki i obywatele Unii są zainteresowani postępem wdrażania rozwiązań technologii cyfrowych, które uproszczą procedury administracyjne niezbędne w kontaktach z władzami lub w codziennym życiu społecznym. Niniejsza opinia ma na celu zwiększenie świadomości krajowych i europejskich decydentów na temat obaw zorganizowanego społeczeństwa obywatelskiego co do potencjalnych negatywnych skutków społecznych przyspieszonego wdrażania technologii cyfrowych.

2.2. Pandemia COVID-19 przyspieszyła transformację cyfrową społeczeństw i zmusiła obywateli do korzystania z nowych technologii w pracy, do nauki i do innych codziennych czynności. Stworzyła możliwości cyfrowego rozwoju dla przedsiębiorstw i obywateli.

2.3. Korzyści płynące z powszechnego wdrożenia tożsamości cyfrowej są szeroko opisywane w różnorakich dokumentach instytucji europejskich i światowych organizacji międzynarodowych. Najnowszym dokumentem w tej kwestii jest wniosek dotyczący rozporządzenia w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej ([1]), opublikowany 3 czerwca 2021 r.

2.4. Komisja Europejska dąży do stworzenia europejskich ram tożsamości cyfrowej w oparciu o przegląd obecnie obowiązujących ram, tak aby do 2030 r. co najmniej 80 % obywateli miało możliwość korzystania z rozwiązania w zakresie identyfikacji elektronicznej, aby mieć dostęp do kluczowych usług publicznych ([2]). Organy sektora publicznego muszą dysponować odpowiednimi zasobami ludzkimi i finansowymi, aby móc wykorzystywać i kontrolować rozwój technologii cyfrowych.

2.5. Dowodzi tego opublikowany przez Komisję Europejską w 2021 r. indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) ([3]), który pokazuje, że w 2020 r. odsetek osób posiadających przynajmniej podstawowe umiejętności cyfrowe wynosił 56 %. Niemniej jednak mimo że większość miejsc pracy wymaga podstawowych umiejętności cyfrowych, duża część mieszkańców UE jeszcze ich nie ma. Wielu obywateli twierdzi, że ma umiejętności cyfrowe, ale po bliższej analizie nie są one niczym więcej niż zdolnością podstawowego korzystania z możliwości oferowanych przez internet (przeglądanie stron internetowych i portali społecznościowych) oraz pakietów oprogramowania oferowanych przez Microsoft Office lub Mac OS.

2.6. Opublikowane niedawno przez Europejski Bank Inwestycyjny badanie dotyczące sztucznej inteligencji ([4]) pokazuje, że Europa wciąż pozostaje w tyle za innymi światowymi potęgami gospodarczymi. Wspomina się w nim, że na USA i Chiny przypada łącznie ponad 80 % z 25 mld EUR rocznych inwestycji kapitałowych w AI i technologie blockchain. Na UE przypada zaledwie 7 %, a całkowita luka inwestycyjna wynosi 5–10 mld EUR rocznie.

2.7. Komisja zaproponowała wypełnienie tej luki i przeznaczenie 1 mld EUR rocznie na inwestycje w AI, które powinny być uzupełnione inwestycjami prywatnymi i środkami własnymi państw członkowskich. Celem jest osiągnięcie 20 mld EUR inwestycji rocznie w ciągu najbliższej dekady ([5]).

3. **Uwagi ogólne**

3.1. Postęp technologiczny ogółem i ewolucja technologii cyfrowych, biotechnologii i systemów łączności elektronicznej w ciągu ostatnich dwudziestu lat stworzyły na całym świecie ogromne możliwości konsolidacji zamożnych, bardziej zintegrowanych i sprawiedliwych społeczeństw.

3.2. Jednocześnie, bez nowej umowy społecznej i ram prawnych dostosowanych do tych nowych technologii o potencjale zakłócającym, pojawia się wiele zagrożeń dla ludzkości (takich jak utrata miejsc pracy spowodowana rozwojem i wdrażaniem automatyzacji, naruszanie prywatności, stronniczość algorytmiczna spowodowana nieprawidłowymi danymi, niestabilność rynków itp.). Należy przy tym pamiętać zwłaszcza o nieustannych próbach narzucania własnych produktów i usług przez globalnych gigantów technologicznych, którzy omijają obowiązujące na poziomie międzynarodowym i krajowym prawodawstwo gwarantujące podstawowe prawa człowieka.

3.3. Międzynarodowe i krajowe instytucje rządowe są podatne na działania podmiotów niepaństwowych mających bezpośredni dostęp do wiedzy, patentów, technologii i funduszy inwestycyjnych, ponieważ pracownicy tych instytucji często nie są w stanie zrozumieć pełnego społecznego wpływu nowych technologii na prawa obywateli i konsumentów. Komitet jest przekonany, że we wszystkich przyszłych działaniach politycznych należy uwzględniać kwestie suwerenności technologicznej UE.

([1]) Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (COM(2021) 281 final).

([2]) Tożsamość cyfrowa dla wszystkich Europejczyków.

([3]) https://digital-strategy.ec.europa.eu/pl/node/9773

([4]) Badanie EBI, *Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy* [Sztuczna inteligencja, blockchain i przyszłość Europy. Jak przełomowe technologie tworzą możliwości dla zielonej gospodarki i gospodarki cyfrowej].

([5]) Komisja Europejska – Europejskie podejście do sztucznej inteligencji.

3.4. EKES domaga się, aby przepisy doprecyzowano i uzupełniono o wyraźne i mające pełne zastosowanie regulacje oraz wspólne normy we wszystkich państwach członkowskich, w tym o powiązane obowiązki, w związku z faktem, że technologiami związanymi z tożsamością cyfrową w dużej mierze zarządzają algorytmy komputerowe i sztuczna inteligencja, które nie mogą ponosić odpowiedzialności za popełniane przez siebie błędy.

3.5. Istnieje już wiele udowodnionych i dokładnie zbadanych sytuacji, w których ludzie ponoszą konsekwencje błędnych decyzji algorytmów komputerowych i sztucznej inteligencji i są za nie niesprawiedliwie skazywani. Na przykład osoby podejmujące decyzje w siłach bezpieczeństwa i policji opierają się na błędnych wynikach działania algorytmów komputerowych takich jak sztuczna inteligencja, rozpoznawanie twarzy, uczenie maszynowe, analiza danych i prognozowanie, arkusze czasu pracy i wyniki itp. Skutkiem tego jest naruszenie praw i wolności wielu obywateli.

3.6. Dlatego też przepisy prawne, które mają objąć dziedzinę tożsamości cyfrowej i związane z nią technologie, muszą opierać się przede wszystkim na pełnej przejrzystości, prawidłowym i pełnym informowaniu użytkowników oraz dobrowolnej świadomej zgodzie, a także zapewniać pełną ochronę, która uwzględni podatność na zagrożenia w cyberprzestrzeni charakteryzującą sieci łączności ruchomej i ich urządzenia itp. Z tych powodów EKES nalega, aby wszystkie sektory wykorzystujące dane osobowe i biometryczne, takie jak tożsamość cyfrowa, sieci łączności ruchomej 5G, sztuczna inteligencja itp., były regulowane w sposób wyraźny, przejrzysty i w pełni zgodny z podstawowymi prawami człowieka.

4. **Uwagi szczegółowe**

Tożsamość cyfrowa

4.1. Jeśli chodzi o wdrażanie identyfikacji elektronicznej w Europie, zarządzanie danymi ma zasadnicze znaczenie dla zapewnienia ochrony obywateli i zabezpieczenia ich prywatności. Należy zapewnić pełną zgodność z ogólnym rozporządzeniem o ochronie danych (RODO).

4.2. Obywatele Unii znajdują się w centrum wszelkich programów i strategii realizowanych w UE. Komitet docenia i popiera opublikowanie wniosku Komisji w sprawie tożsamości cyfrowej dla wszystkich Europejczyków ([6]), w którym stwierdza się, że decyzja o stosowaniu lub niestosowaniu identyfikacji elektronicznej musi należeć do danej osoby. Uważa jednak, że bagatelizuje się skutki wykluczenia niektórych obywateli, którzy nie zdecydują się na posiadanie identyfikacji elektronicznej, i nalega, aby prawo do bycia zapomnianym i do bycia offline zostało wyraźnie wdrożone w prawodawstwie UE.

4.3. EKES wzywa do wprowadzenia jasnych przepisów antydyskryminacyjnych we wszystkich przyszłych wnioskach ustawodawczych dotyczących tego zagadnienia. Bez względu na powód, dla którego obywatel zdecydowałby się nie korzystać z takiej funkcji (czy to ze względu na ochronę danych, czy anonimowość, czy też z innych powodów), nie można stawiać go w gorszej sytuacji niż aktywnych użytkowników ani marginalizować. Dane osobowe powinny zawsze pozostawać własnością danej osoby, a podstawą wdrażania identyfikacji elektronicznej musi być ochrona praw człowieka. Z myślą o zagwarantowaniu ochrony i bezpieczeństwa danych, a także poszanowania życia prywatnego Komitet proponuje, aby tożsamością cyfrową obywateli UE zarządzał w każdym państwie członkowskim organ administracji publicznej, podlegający zwierzchnictwu państwa oraz demokratycznej kontroli parlamentów narodowych.

4.4. Wprowadzenie identyfikacji elektronicznej w Europie powinno mieć na celu umożliwienie konsumentom bezpiecznej i łatwej łączności. Musi zapewniać między innymi poprawę jakości danych i świadczenia usług publicznych, wzmocnienie ukierunkowanych programów rządowych oraz większą efektywność rynku kredytowego. EKES popiera taki scenariusz. Zauważa jednak, że wdrożenie identyfikacji elektronicznej pociąga za sobą szereg zagrożeń w zakresie ochrony prywatności i danych, i całkowicie sprzeciwia się wprowadzeniu systemu, który umożliwia dokładną obserwację obywateli Unii, ich śledzenie i/lub monitorowanie ich działań i zachowań.

4.5. Cyberbezpieczeństwo jest ważnym aspektem wdrożenia, ponieważ ryzyko zhakowania istotnych danych osobowych i finansowych jest wysokie. EKES ma nadzieję, że ostateczna wersja proponowanych przepisów oraz porozumienie między państwami członkowskimi w sprawie norm, specyfikacji technicznych i aspektów interoperacyjności będą gotowe do października 2022 r. EKES uważa, że zorganizowane społeczeństwo obywatelskie, w tym partnerzy społeczni, organizacje pozarządowe i środowiska akademickie, muszą w pełni uczestniczyć w procesie wdrażania.

([6]) Tożsamość cyfrowa dla wszystkich Europejczyków (COM(2021) 281 final).

4.6. Jednym z największych zagrożeń związanych z wdrożeniem identyfikacji elektronicznej są oszustwa. Wiadomości wyłudzających informacje, które wszyscy dziś otrzymujemy, będzie jeszcze więcej, a ich celem będą najsłabsze grupy w Europie. EKES jest zdania, że kwestie bezpieczeństwa w tym zakresie nie zostały wystarczająco dokładnie określone ilościowo, i jest rozczarowany, że bezpieczeństwo przyszłego cyfrowego portfela nie jest najistotniejszą kwestią we wniosku KE ustanawiającym europejskie ramy tożsamości cyfrowej. Oszustwa z wykorzystaniem syntetycznej tożsamości zdarzały się w innych częściach świata, gdzie wprowadzono podobne systemy, i UE powinna zapoznać się z tymi kwestiami i zająć się nimi przed wdrożeniem identyfikacji elektronicznej. Dlatego Komitet uważa, że bezpieczeństwo danych nie powinno podlegać negocjacjom.

AI – sztuczna inteligencja

4.7. Aby móc się rozwijać i osiągać postępy, jednolity rynek cyfrowy potrzebuje sztucznej inteligencji. AI opiera się na algorytmach, które wymagają ogromnych ilości danych prywatnych i metadanych. Społeczeństwo musi czerpać korzyści z rozwoju technologicznego i z opartej na algorytmach nauki stosowanej. Przy wdrażaniu technologii AI należy jednak zadbać o to, aby społeczności historycznie zmarginalizowane były w stanie poradzić sobie z tymi programami, a istniejące nierówności społeczne się nie pogłębiały.

4.8. EKES jest pierwszą instytucją europejską, która zaleciła przyjęcie podejścia opartego na ludzkiej kontroli przy współpracy z systemami sztucznej inteligencji ([7]). Komitet potwierdza, że najważniejsze jest, aby ostateczna decyzja należała do człowieka oraz aby człowiek sprawował pełną kontrolę nad procesami decyzyjnymi dotyczącymi rozwoju maszyn.

4.9. Ochrona własności intelektualnej może być wykorzystywana jako argument za nieprzejrzystym rozwojem AI. EKES uważa, że należy znaleźć odpowiednią równowagę między nieujawnianiem tajemnic handlowych a zapewnieniem przejrzystości i możliwości śledzenia rozwoju sytuacji. Ponadto we wszystkich wnioskach ustawodawczych UE dotyczących sztucznej inteligencji należy wyraźnie przewidzieć rozliczalność za jej ewentualne nieprawidłowe działanie, a odpowiedzialność powinna spoczywać na twórcach, programistach, inżynierach AI i prawowitych właścicielach.

4.10. Komitet jest zdania, że technologie AI należy wdrażać w sposób społecznie zrównoważony, z uwzględnieniem praw człowieka, wartości europejskich, równości płci, różnorodności kulturowej, interesów grup defaworyzowanych oraz praw własności intelektualnej.

4.11. Aby mieć pewność, że algorytmy są w pełni zgodne z prawem europejskim i go przestrzegają, konieczne są dalsze postępy w zakresie RODO. Komitet apeluje o opracowanie wspólnych zasad etycznych zapewniających swobodny dostęp do źródłowych kodów algorytmów.

4.12. AI ma potencjał, aby przyczynić się do osiągnięcia celów klimatycznych i środowiskowych, jednak należy wziąć pod uwagę ogromne ilości energii, które zużywa się na potrzeby funkcjonowania tych systemów cyfrowych, a także inne wyzwania dotyczące internalizacji kosztów zewnętrznych. EKES proponuje wzmocnienie monitorowania tego aspektu i wzywa przedsiębiorstwa cyfrowe, aby poczyniły postępy w ograniczaniu emisji dwutlenku węgla.

4.13. W kluczowych obszarach, takich jak obrona czy cyberbezpieczeństwo, należy zagwarantować kontrolę ludzi nad robotami. EKES wnosi, aby na szczeblu UE stworzono bardzo precyzyjne ramy, które pozwolą to zapewnić. Zwraca też uwagę, że interwencja człowieka musi być zawsze możliwa w celu usunięcia błędów zautomatyzowanego systemu podejmowania decyzji.

4.14. EKES jest całkowicie przeciwny prywatnym bazom danych służącym rozpoznawaniu twarzy (z wyjątkiem zastosowań związanych z przestępczością) oraz wszelkim rodzajom systemów scoringu obywateli, ponieważ naruszają one podstawowe wartości i prawa UE.

4.15. Jeśli chodzi o aspekty społeczne, EKES jest zaniepokojony, że rozwój sztucznej inteligencji będzie miał ogromny wpływ na rynki pracy, powodując potencjalnie kryzys bezrobocia. Ponadto może wpływać na ludzkie zachowanie i prowadzić do lenistwa i powierzchowności.

([7]) Dz.U. C 288 z 31.8.2017, s. 1.

Duże zbiory danych

4.16. EKES z zadowoleniem przyjmuje akt w sprawie danych ([8]) wydany przez Komisję Europejską w lutym 2022 r. i uważa, że stanowi on etyczne ramy przejrzystego przetwarzania danych osobowych, przy zachowaniu pełnej kontroli przez obywateli i przedsiębiorstwa, którzy je generują. Umożliwia także wykorzystanie danych przez większą liczbę zainteresowanych stron i obywateli, co przynosi szersze korzyści konsumentom, przedsiębiorstwom i organom sektora publicznego, a tym samym prowadzi do powstania sprawiedliwej gospodarki opartej na danych.

4.17. Duże ilości danych są obecnie dostępne dla organów sektora publicznego i kilku gigantów technologicznych, takich jak Google, Facebook (Meta), TikTok czy Amazon. Niestety korzysta z nich teraz tylko ograniczona liczba zainteresowanych stron i EKES jest zaniepokojony, że dane pochodzące z UE są przechowywane, przetwarzane i przynoszą wartość poza Europą ([9]). Komitet uważa, że trudno będzie osiągnąć suwerenność cyfrową UE bez posiadania własnych gigantów technologii cyfrowej w UE, bez przechowywania europejskich danych na terytorium UE i bez ochrony tych danych przed jakimkolwiek dostępem z zewnątrz.

4.18. Zarządzanie dużymi zbiorami danych musi zawsze odbywać się z poszanowaniem praw człowieka zapisanych w art. 21 Karty praw podstawowych Unii Europejskiej ([10]), zwłaszcza gdy w procesie podejmowania decyzji wykorzystuje się algorytmy. Dostawcy usług w chmurze z UE stanowią jedynie niewielką część międzynarodowego rynku, który jest w dużej mierze zdominowany przez przedsiębiorstwa z USA. Stawia to UE w niekorzystnej sytuacji i ogranicza możliwości inwestycyjne na rynku przetwarzania danych. Utrudnia to też konkurencyjność dużych przedsiębiorstw oraz ich możliwości rozwoju i zdobywania rynków, a także uniemożliwia małym i średnim przedsiębiorstwom zwiększanie skali działalności. Komitet z zadowoleniem przyjmuje komunikat Komisji Europejskiej pt. „Polityka konkurencji gotowa na nowe wyzwania" ([11]) oraz wagę, jaką przywiązuje się do transformacji cyfrowej przy kształtowaniu przyszłych unijnych ram konkurencji.

4.19. Komitet uważa, że świadoma zgoda na wykorzystanie danych musi być udzielana w odniesieniu zarówno do danych osobowych, jak i nieosobowych. EKES ponownie wzywa do ulepszenia RODO pod tym względem.

Sprawiedliwa transformacja cyfrowa i umiejętności cyfrowe w UE

4.20. Komitet zauważa, że rynek pracy się zmienia i coraz więcej sektorów gospodarki skarży się na brak wykwalifikowanej i kompetentnej siły roboczej. Odnotowuje również spadek kwalifikacji oraz brak know-how i wiedzy fachowej.

4.21. W poprzednich opiniach EKES wzywał do stworzenia Unii, w której włączenie cyfrowe jest powszechne i nikt nie jest pozostawiony w tyle. Lata później nierówności między państwami członkowskimi pogłębiają się, a słabsze grupy społeczne nadal nie są objęte ochroną, zwłaszcza osoby starsze, które są najbardziej narażone.

4.22. Komitet wyraża zaniepokojenie istniejącą przepaścią cyfrową w UE i wzywa do skoordynowanego wdrażania programów rozwoju umiejętności cyfrowych we wszystkich państwach członkowskich oraz do urzeczywistnienia w UE idei cyfrowego uczenia się przez całe życie, w tym rozwiązań opartych na otwartym oprogramowaniu jako bezpłatnej alternatywy dla komercyjnych. Kształtowanie umiejętności cyfrowych rozpoczyna się od kursów słownictwa, a kończy na praktycznych szkoleniach.

4.23. Zaangażowanie pracowników w proces transformacji cyfrowej jest niezbędne, aby mogli oni zrozumieć zarówno przyszłe zagrożenia, jak i możliwości. Zmieniające się środowisko pracy wymaga transferu wiedzy i nabywania nowych umiejętności, ale także poprawy warunków pracy osób pracujących za pośrednictwem cyfrowych platform pracy.

4.24. EKES wzywa do tworzenia silnego europejskiego systemu edukacji cyfrowej, który może przygotować siłę roboczą do wyzwań technologicznych i pomóc jej w zdobyciu miejsc pracy wysokiej jakości, i przypomina w związku z tym o umowie ramowej europejskich partnerów społecznych w sprawie cyfryzacji.

([8]) Komisja Europejska – Akt w sprawie danych.

([9]) Eurostat podaje, że w 2020 r. tylko 36 % unijnych przedsiębiorstw korzystało z usług w chmurze – większość z nich do obsługi poczty elektronicznej i przechowywania danych, wykorzystując w tym celu moce tylko 19 % dostawców takich usług.

([10]) Dz.U. C 326 z 26.10.2012, s. 391.

([11]) Komunikat KE „Polityka konkurencji gotowa na nowe wyzwania" (COM(2021) 713 final).

4.25. Komitet apelował już o dalszą poprawę solidnych kompetencji w dziedzinie nauk ścisłych, technologii, inżynierii i matematyki ([12]).

Bruksela dnia 14 lipca 2022 r.

Christa SCHWENG
Przewodnicząca
Europejskiego Komitetu Ekonomiczno-Społecznego

([12]) Dz.U. C 14 z 15.1.2020, s. 46; Dz.U. C 10 z 11.1.2021, s. 40; Dz.U. C 228 z 5.7.2019, s. 16; Dz.U. C 75 z 10.3.2017, s. 6; Dz.U. C 374 z 16.9.2021, s. 11.