III

(Akty przygotowawcze)

EUROPEJSKI KOMITET EKONOMICZNO-SPOŁECZNY

547. SESJA PLENARNA EKES-U, 30.10.2019–31.10.2019

Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów »Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka«"

[COM(2019) 168 final]

(2020/C 47/09)

Sprawozdawczyni: **Franca SALIS-MADINIER**

Wniosek o sporządzenie opinii	Komisja Europejska, 3.6.2019
Podstawa prawna	Art. 304 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Jednolitego Rynku, Produkcji i Konsumpcji
Data przyjęcia przez sekcję	18.10.2019
Data przyjęcia na sesji plenarnej	30.10.2019
Sesja plenarna nr	547
Wynik głosowania (za/przeciw/wstrzymało się)	198/1/4

1. Wnioski i zalecenia

1.1. Sztuczna inteligencja (SI) nie jest celem samym w sobie, lecz narzędziem, które może spowodować radykalne pozytywne przemiany, ale jednocześnie niesie ze sobą pewne ryzyko. Dlatego też należy stworzyć ramy korzystania z niej.

1.2. Komisja powinna przedsięwziąć środki mające na celu przewidywanie niewłaściwego wykorzystywania SI oraz uczenia się maszyn, zakazywanie tego rodzaju praktyk oraz zapobieganie im. Powinna także lepiej uregulować wprowadzanie na rynek produktów, które mogą zostać wykorzystane w złej intencji.

1.3. Komisja powinna zwłaszcza propagować rozwój systemów SI ukierunkowanych na konkretne zastosowania, które pozwoliłyby przyspieszyć transformację ekologiczną i klimatyczną.

1.4. Konieczne jest określenie, które wyzwania można rozwiązać za pomocą kodeksów etycznych, samoregulacji i dobrowolnych zobowiązań, a które za pomocą środków regulacyjnych i prawnych uzupełnionych o monitorowanie i – w przypadku niezgodności – sankcje. W każdym przypadku systemy sztucznej inteligencji muszą być zgodne z obowiązującym prawodawstwem.

1.5. SI wymaga podejścia obejmującego aspekty techniczne, lecz również szersze aspekty społeczne i etyczne. EKES przyjmuje z zadowoleniem chęć opracowania przez UE ukierunkowanego na człowieka podejścia do SI zgodnego z leżącymi u jej podstaw wartościami: poszanowaniem godności ludzkiej, wolnością, demokracją, równością i niedyskryminacją, praworządnością i poszanowaniem praw człowieka.

1.6. EKES potwierdza ([1]) potrzebę informowania pracowników i ich przedstawicieli oraz przeprowadzania z nimi konsultacji podczas wprowadzania systemów SI mogących zmienić organizację pracy, w tym nadzór i kontrolę, a także systemów oceny i naboru pracowników. Komisja powinna propagować dialog społeczny w celu włączenia pracowników w zastosowanie systemów SI.

([1]) Dz.U. C 440 z 6.12.2018, s. 1.

1.7. EKES podkreśla ([2]), że godna zaufania SI zakłada kontrolę człowieka nad maszyną i informowanie obywateli o zastosowaniu systemów SI. Systemy te powinny być możliwe do wyjaśnienia lub, gdy nie jest to możliwe, należy dostarczać obywatelom i konsumentom informacji o ograniczeniach i zagrożeniach związanych z tymi systemami.

1.8. UE musi zaradzić „pojawiającym się zagrożeniom" ([3]) w dziedzinie bezpieczeństwa i higieny pracy. Niezbędne jest opracowanie przepisów w celu niedopuszczenia do tego, by automatyczne systemy przynosiły szkodę lub wyrządzały krzywdę człowiekowi. Należy przeszkolić pracowników w zakresie współpracy z maszyną i jej unieruchomienia w nagłych przypadkach.

1.9. EKES opowiada się za stworzeniem solidnego systemu certyfikacji opartego na procedurach testowych, które umożliwiałyby przedsiębiorstwom potwierdzenie wiarygodności i bezpieczeństwa swych systemów SI. Przejrzystość, identyfikowalność i wytłumaczalność procesu podejmowania decyzji w oparciu o algorytm to wciąż wyzwania techniczne, które wymagają wsparcia w postaci instrumentów UE takich jak program „Horyzont Europa".

1.10. Ochrona prywatności i danych osobowych określi poziom zaufania obywateli i konsumentów do SI. Własność danych, ich kontrola i wykorzystanie przez przedsiębiorstwa i organizacje to kwestie, które należy jeszcze w dużej mierze uregulować (w szczególności w odniesieniu do internetu rzeczy). EKES zachęca Komisję, by w świetle rozwoju technologii dokonywała regularnego przeglądu ogólnego rozporządzenia o ochronie danych (RODO) ([4]) i związanych z nim przepisów.

1.11. Zdaniem EKES-u niezbędne jest rozważenie wkładu, jaki systemy SI mogą wnieść w ograniczanie emisji gazów cieplarnianych, zwłaszcza w sektorach przemysłu, transportu, energii, budownictwa i rolnictwa. Apeluje, by kwestie zmiany klimatu i transformacji cyfrowej były rozważane wspólnie.

1.12. EKES uważa, że kontrola systemów SI może być niewystarczająca do określenia zakresu odpowiedzialności i wzbudzenia zaufania. Komitet zaleca, by nadać priorytet stworzeniu jasnych przepisów, które w wypadku niespełnienia zasad obarczałyby odpowiedzialnością podmioty posiadające osobowość prawną: osoby fizyczne lub prawne. Wzywa również Komisję do zbadania w trybie priorytetowym podstawowej kwestii, jaką jest możliwość ubezpieczania systemów SI.

1.13. EKES proponuje – dla przedsiębiorstw spełniających normy – opracowanie „europejskiego certyfikatu zaufanego przedsiębiorstwa w sektorze sztucznej inteligencji", w oparciu między innymi o listę oceniającą zaproponowaną przez grupę ekspertów wysokiego szczebla ds. SI.

1.14. Promując odpowiednie prace w ramach grup G-7 i G-20 oraz w ramach dialogu dwustronnego, UE musi dążyć do zapewnienia, by uregulowania w sprawie sztucznej inteligencji wykraczały poza granice europejskie. Konieczne jest stworzenie międzynarodowego porozumienia w sprawie godnej zaufania sztucznej inteligencji, które umożliwi opracowanie międzynarodowych norm i regularne sprawdzanie ich adekwatności.

2. **Streszczenie wniosku Komisji**

2.1. Omawiany komunikat opiera się na pracach grupy ekspertów wysokiego szczebla, którą Komisja powołała w czerwcu 2018 r. Komisja określiła w nim siedem kluczowych wymogów, wymienionych w pkt 4, w celu zapewnienia SI godnej zaufania.

2.2. Komisja rozpoczęła fazę pilotażową z udziałem wielu różnych zainteresowanych stron. Skoncentrowano się zwłaszcza na liście kontrolnej, którą grupa ekspertów wysokiego szczebla sporządziła w odniesieniu do każdego z zasadniczych wymogów. Na początku 2020 r. grupa wysokiego szczebla dokona przeglądu i aktualizacji tej listy, a Komisja zaproponuje, w razie konieczności, nowe środki.

2.3. Komisja pragnie zastosować swoje podejście do sztucznej inteligencji na arenie międzynarodowej i będzie nadal odgrywać aktywną rolę, w tym w ramach grup G-7 i G-20.

([2]) Dz.U. C 288 z 31.8.2017, s. 1, Dz.U. C 440 z 6.12.2018, s. 1.

([3]) https://osha.europa.eu/en/emerging-risks

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

3. Uwagi ogólne

3.1. SI ukierunkowana na człowieka wymaga podejścia obejmującego aspekty techniczne, lecz również społeczne i etyczne. EKES przyjmuje z zadowoleniem chęć opracowania przez instytucje UE podejścia do SI zgodnego z leżącymi u jej podstaw wartościami: poszanowaniem godności ludzkiej, wolnością, demokracją, równością i niedyskryminacją, praworządnością i poszanowaniem praw człowieka. Jak podkreśla Komisja ([5]), SI nie jest celem samym w sobie, lecz narzędziem, które może przynieść radykalne pozytywne zmiany. Tak jak wszystkie narzędzia stwarza zarówno możliwości, jak i zagrożenia. Dlatego też UE powinna ustalić ramy korzystania z niej i jasno określić zakres odpowiedzialności.

3.2. Zaufanie do SI ukierunkowanej na człowieka narodzi się z potwierdzenia wartości i zasad, z jasno określonych ram regulacyjnych i wytycznych w dziedzinie etyki obejmujących zasadnicze wymogi.

3.3. Niezbędne jest rozpoznanie – z udziałem wszystkich zainteresowanych stron – wśród licznych wyzwań związanych z SI tych, którym będzie trzeba stawić czoła za pomocą środków regulacyjnych i legislacyjnych połączonych z ustalonymi w przepisach mechanizmami monitorowania i – w wypadku ich nieprzestrzegania – z sankcjami, a także wyzwań, którym będzie można sprostać za pomocą kodeksu etycznego, samoregulacji i dobrowolnych zobowiązań. EKES z zadowoleniem zauważa, że Komisja uwzględniła pierwotnie poruszone przez niego zasady, lecz ubolewa, że na tym etapie nie proponuje konkretnych środków mających na celu rozproszenie uzasadnionych obaw w dziedzinie praw konsumentów, bezpieczeństwa systemów i odpowiedzialności.

3.4. Systemy SI muszą być zgodne z obowiązującymi ramami prawnymi, w szczególności w odniesieniu do ochrony danych osobowych, odpowiedzialności za produkt, ochrony konsumentów, niedyskryminacji, kwalifikacji zawodowych oraz informowania pracowników i przeprowadzania z nimi konsultacji w miejscu pracy. Należy zapewnić dostosowanie tych przepisów do nowych wyzwań związanych z cyfryzacją i SI.

3.5. Jak zauważa Komisja, „Należy wprowadzić procedury mające na celu wyjaśnienie i ocenę potencjalnych zagrożeń związanych ze stosowaniem systemów SI w różnych obszarach zastosowań" ([6]). EKES przywiązuje największą wagę do przyszłych metod tej oceny, a także do opracowania wskaźników, które mogłyby zostać uwzględnione w celu przeprowadzenia oceny. Projekt listy kontrolnej sporządzonej przez grupę ekspertów wysokiego szczebla jest punktem wyjścia do wdrażania takich procedur.

3.6. Dotyczy to również kwestii sprawiedliwego podziału oczekiwanej wartości dodanej systemów SI. EKES uważa, że pozytywne przemiany, które niesie ze sobą SI w dziedzinie rozwoju gospodarczego, zrównoważonego charakteru procesów produkcji i konsumpcji (w szczególności energii) i poprawy wykorzystania zasobów, powinny być korzystne dla wszystkich krajów, a w ich obrębie – dla wszystkich obywateli.

4. Uwagi szczegółowe

4.1. *Przewodnia i nadzorcza rola człowieka*

4.1.1. Komisja pragnie zagwarantować, że korzystanie z systemów sztucznej inteligencji w żadnym wypadku nie podważy niezależności ludzkiej ani nie spowoduje negatywnych skutków. EKES zgadza się z podejściem opartym na kontroli człowieka nad maszyną, tak jak stwierdził już w swych wcześniejszych opiniach.

4.1.2. W związku z tym konieczne jest, by obywatele byli prawidłowo informowani o wykorzystaniu systemów SI, by systemy te były możliwe do objaśnienia lub – jeżeli nie jest to możliwe (np. w wypadku głębokiego uczenia maszynowego) – by użytkownicy otrzymywali informacje o ograniczeniach i zagrożeniach związanych z systemem. W każdym wypadku obywatele powinni zachować swobodę podejmowania decyzji innych niż SI.

4.1.3. W przedsiębiorstwach publicznych i administracji publicznej pracownicy i ich przedstawiciele muszą być należycie informowani i konsultowani podczas wprowadzania systemów sztucznej inteligencji, które mogą zmienić organizację pracy i wpływać na kontrolę, monitorowanie, ocenę i rekrutację pracowników. Komisja powinna propagować dialog społeczny w celu włączenia pracowników w zastosowanie systemów SI.

4.1.4. Co się tyczy zasobów ludzkich, szczególną uwagę trzeba poświęcić ryzyku nadużywania systemów SI (na przykład do nieograniczonego nadzoru, gromadzenia danych osobowych, danych dotyczących zdrowia, wymiany danych z osobami trzecimi), a także ryzyku pojawiającemu się w dziedzinie bezpieczeństwa i higieny pracy ([7]). Niezbędne jest ustanowienie jasnych przepisów w celu niedopuszczenia do sytuacji, w której współpraca między człowiekiem a maszyną doprowadziłaby do szkód dla ludzi. Norma ustanowiona przez Międzynarodową Organizację Normalizacyjną (ISO) w odniesieniu do robotów współpracujących ([8]), które dotyczą producentów, podmiotów zajmujących się integracją technologii i użytkowników, dostarcza wytycznych w sprawie tworzenia i organizacji przestrzeni roboczej oraz ograniczenia ryzyka, na które mogą zostać narażone poszczególne osoby. Pracownicy powinni zostać przeszkoleni w zakresie stosowania SI i robotyki, współpracy z nimi, a zwłaszcza – umiejętności ich unieruchomienia w nagłej sytuacji (zasada „hamulca bezpieczeństwa").

([5]) COM(2019) 168 final.
([6]) COM(2019) 168 final, s. 5.
([7]) Zob. w szczególności „BHP i przyszłość pracy. Korzyści i ryzyko związane ze stosowaniem narzędzi sztucznej inteligencji w miejscu pracy"
([8]) ISO/TS 15066, 2016 r.

4.2. *Techniczna solidność i bezpieczeństwo*

4.2.1. EKES opowiada się za stworzeniem europejskich standardów ochrony oraz solidnego systemu certyfikacji opartego na procedurach badawczych, które umożliwiałyby przedsiębiorstwom potwierdzenie wiarygodności swych systemów SI. EKES pragnie również podkreślić znaczenie kwestii możliwości ubezpieczania systemów SI.

4.2.2. Komisja w niewielkim stopniu porusza kwestię przewidywania szkodliwego zastosowania SI i uczenia się maszyn, przed którym przestrzega wielu badaczy ([9]), a także zapobiegania mu i jego zakazu. Korzystne byłoby uwzględnienie zaleceń badaczy, zwłaszcza w odniesieniu do dwojakiego zastosowania technologii, które może dotyczyć bezpieczeństwa cyfrowego (rozpowszechnienia ataków cybernetycznych, wykorzystywania słabości ludzi i SI oraz *data poisoning*), bezpieczeństwa fizycznego (hakowanie autonomicznych systemów, w tym pojazdów autonomicznych, dronów i broni automatycznej) czy też bezpieczeństwa politycznego (masowe gromadzenie danych osobowych, ukierunkowana propaganda, manipulacja wideo itp.). Badacze, inżynierowie i organy publiczne muszą ściśle ze sobą współpracować w celu zapobieżenia ryzyku. Eksperci i inne zainteresowane strony, w tym użytkownicy i konsumenci, powinni mieć możliwość udziału w dyskusjach na temat tych wyzwań.

4.3. *Ochrona prywatności i danych*

4.3.1. Komisja opowiada się za tym, by dostępem do danych właściwie zarządzano i by był on kontrolowany ([10]). EKES uważa, że trzeba wyjść poza ogólniki. Stopień zaufania obywatela do systemów SI będzie decydował również o ich rozwoju. Do uregulowania w dużej mierze pozostają takie kwestie jak własność danych, ich kontrola i wykorzystanie przez przedsiębiorstwa i organizacje. Wątpliwości budzi na przykład ilość i rodzaj danych przekazywanych przez samochody producentom samochodów ([11]). Pomimo zasady „uwzględnienia ochrony prywatności już w fazie projektowania", którą na mocy RODO spełniać muszą skomunikowane urządzenia, trzeba stwierdzić, że konsumenci dysponują bardzo ograniczonymi informacjami na ten temat bądź w ogóle ich nie posiadają i że nie ma żadnego sposobu, by dane te kontrolować. Dlatego też EKES wzywa Komisję, by w świetle rozwoju technologii dokonała przeglądu RODO i związanych z tym rozporządzeniem przepisów ([12]).

4.4. *Przejrzystość*

4.4.1. EKES uważa, że wytłumaczalność procesu podejmowania decyzji w oparciu o algorytm jest niezbędna do zrozumienia nie mechanizmów jako takich, lecz logiki procesów podejmowania decyzji, a także sposobu, w jaki systemy SI na nie wpływają. Opracowanie standardowych procedur badawczych dla systemów uczenia maszynowego (*machine learning*) pozostaje wyzwaniem technicznym i wymaga wsparcia takich instrumentów UE jak program „Horyzont Europa".

4.4.2. EKES zgadza się z podejściem Komisji, wedle którego „systemy SI powinny być rozpoznawalne jako takie, zapewniając, że użytkownicy będą świadomi tego, że wchodzą w interakcje z systemem SI" ([13]), również w ramach relacji między pacjentem a pracownikiem służby zdrowia oraz w ramach profesjonalnych usług związanych ze zdrowiem i dobrostanem obywateli. EKES podkreśla również, że użytkownik lub konsument musi być też informowany o usługach świadczonych przez człowieka. Liczne systemy SI wymagają de facto dużego nakładu pracy ludzkiej, często niewidocznej dla użytkowników końcowych ([14]). Wiąże się z tym wyzwanie braku przejrzystości wobec użytkowników i konsumentów usług, a także pewna forma wykorzystania pracy ukrytej i nieuznanej.

4.4.3. Ponadto EKES uważa, że konsument powinien być stale informowany o systemach SI wbudowanych w nabywane przez siebie produkty i musi mieć nieprzerwanie możliwość dostępu do swoich danych i ich kontroli.

4.5. *Różnorodność, niedyskryminacja i sprawiedliwość*

4.5.1. Ryzyko dyskryminacji dotyczy niektórych zastosowań SI umożliwiających modelowanie profili obywateli, użytkowników i konsumentów (na przykład w celu naboru, wynajmu nieruchomości, niektórych usług na rzecz osób itp.). UE posiada szereg przepisów prawnych dotyczących równego traktowania i niedyskryminacji ([15]). Systemy SI muszą być z nimi zgodne. Prawodawstwo to musi jednak również zostać dostosowane i, w razie konieczności, wzmocnione (w tym na poziomie egzekwowania), by uwzględnić nowe praktyki. Istnieje rzeczywiste ryzyko, że profilowanie algorytmiczne stanie się nowym potężnym narzędziem dyskryminacji. UE musi zapobiec temu ryzyku.

([9]) Zob. sprawozdanie: „*The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*" („Korzystanie ze sztucznej inteligencji w złych zamiarach: prognozowanie, zapobieganie i łagodzenie"), luty 2018 r.

([10]) COM(2019) 168 final, s. 6.

([11]) „*Your car knows when you gain weight*", The New York Times (wydanie międzynarodowe), 22 maja 2019 r.

([12]) Dz.U. C 190 z 5.6.2019, s. 17.

([13]) COM(2019) 168 final, s. 6.

([14]) Zob. na przykład: „*A white-collar sweatshop': Google Assistant contractors allege wage theft*", The Guardian, 29 maja 2019 r. i „*Bot technology impressive, except when it's not the bot*", The New York Times (wydanie międzynarodowe), 24 maja 2019 r.

([15]) Dz.U. L 180 z 19.7.2000, s. 22, Dz.U. L 303 z 2.12.2000, s. 16, Dz.U. L 373 z 21.12.2004, s. 37, Dz.U. L 204 z 26.7.2006, s. 23.

4.5.2. Dyrektywa w sprawie przeciwdziałania rasizmowi ([16]) oraz dyrektywa w sprawie równego traktowania kobiet i mężczyzn poza środowiskiem pracy ([17]) przewidują powołanie specjalnych i kompetentnych organów ds. promowania równości kobiet i mężczyzn. EKES wzywa, by organy te odgrywały aktywną rolę w monitorowaniu i kontroli systemów SI w związku z ryzykiem bezpośredniej lub pośredniej dyskryminacji.

4.6. *Dobrostan społeczny i środowiskowy*

4.6.1. Komisja nie przedstawiła konkretnych sposobów wzajemnego połączenia transformacji klimatycznej z transformacją cyfrową, w szczególności w zakresie wykorzystania systemów SI. Niezbędne jest rozważenie wkładu, jaki systemy SI mogą wnieść w ograniczanie emisji gazów cieplarnianych, zwłaszcza w sektorach przemysłu, transportu, energii, budownictwa i rolnictwa.

4.6.2. Komisja stwierdza, że systemy SI można wykorzystać do rozwoju umiejętności społecznych, lecz że mogą się one również przyczynić do ich pogorszenia. EKES uważa, że UE musi w większym stopniu uwzględnić niektóre wyzwania społeczne. Badania wykazały na przykład, że projektowanie niektórych aplikacji wyposażonych w systemy sztucznej inteligencji ma na celu maksymalne wydłużanie korzystania przez użytkowników z usług internetowych (z sieci społecznościowych, gier, nagrań wideo itp.). Celem jest umożliwienie gromadzenia maksymalnej ilości danych dotyczących ich zachowań. Strategie te polegają na niekończącym się odnawianiu zaleceń algorytmicznych, przypomnieniach i powiadomieniach, grach itp. Skutki nadmiernego korzystania z sieci i nagabywania dzieci były przedmiotem badań ([18]); wyniki wskazują na wzrost poziomu lęku i agresji, brak snu i wpływ na edukację, stosunki społeczne, zdrowie i dobrostan. Aby tworzyć godną zaufania SI, UE powinna uwzględniać takie skutki i zapobiegać im.

4.6.3. Jeden z czynników dobrostanu społecznego związany jest z poczuciem bezpieczeństwa w pracy. Skutki cyfryzacji mogą zaburzać poczucie bezpieczeństwa i wywoływać stres ([19]). Dlatego też należy opracować strategie antycypowania zmian (zanim dojdzie do ewentualnej restrukturyzacji) i kształcenia ustawicznego wszystkich pracowników. Wymaga to wysokiej jakości dialogu między pracodawcami i przedstawicielami pracowników w przedsiębiorstwach, który umożliwi sprzyjające włączeniu społecznemu zastosowanie nowych technologii, szczególnie SI i robotyki. By zwiększyć zaufanie między kierownictwem a pracownikami, systemy SI dotyczące zarządzania, oceny i kontroli pracowników powinny być wytłumaczalne, ich parametry muszą być znane, a funkcjonowanie – przejrzyste.

4.7. *Odpowiedzialność*

4.7.1. Decyzje podejmowane przez systemy uczenia maszynowego nie są łatwe do wyjaśnienia; ponadto są one regularnie aktualizowane. EKES uważa, że kontrola systemów SI może nie wystarczać do określenia zakresu odpowiedzialności i wzbudzenia zaufania. Dlatego też zaleca stworzenie przepisów, które w wypadku niespełnienia zasad obarczałyby odpowiedzialnością podmioty posiadające osobowość prawną: osoby fizyczne lub prawne. EKES zaleca, by w większym stopniu opierać się na wiarygodnych przedsiębiorstwach lub specjalistach niż na algorytmach i proponuje opracowanie dla przedsiębiorstw, które spełniają wszystkie normy, „europejskiego certyfikatu zaufanego przedsiębiorstwa w sektorze sztucznej inteligencji", w oparciu między innymi o listę oceniającą zaproponowaną przez grupę wysokiego szczebla.

4.7.2. W dyrektywie w sprawie odpowiedzialności za produkty ([20]) ustanowiono zasadę ścisłej odpowiedzialności producentów europejskich: jeżeli produkt mający wadę spowoduje szkodę dla konsumenta, producent może ponosić odpowiedzialność nawet bez winy lub zaniedbania ze swojej strony. Coraz bardziej rozpowszechnione projektowanie, wdrażanie i wykorzystywanie systemów SI wymaga przyjęcia przez UE adekwatnych przepisów dotyczących odpowiedzialności w sytuacjach, gdy produkty zawierające treści cyfrowe i usługi proponowane konsumentom mogą się okazać niebezpieczne lub szkodliwe. Konsumenci powinni mieć dostęp do wymiaru sprawiedliwości w wypadku szkód spowodowanych przez system SI.

5. **Potrzeba uregulowań poza Europą**

5.1. W zglobalizowanym świecie regulacja SI powinna wykraczać poza granice Europy. Europa powinna wspierać szerokie porozumienie dotyczące SI na forum grup G7 i G20 oraz kontynuować rozmowy dwustronne, tak by większość krajów mogła uczestniczyć w procesach normalizacji SI i regularnie kontrolować ich stosowność.

Bruksela, dnia 30 października 2019 r.

Luca JAHIER
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego

([16]) Dyrektywa Rady 2000/43/WE z dnia 29 czerwca 2000 r. wprowadzająca w życie zasadę równego traktowania osób bez względu na pochodzenie rasowe lub etniczne (Dz.U. L 180 z 19.7.2000, s. 22)

([17]) Dyrektywa Rady 2004/113/WE z dnia 13 grudnia 2004 r. wprowadzająca w życie zasadę równego traktowania mężczyzn i kobiet w zakresie dostępu do towarów i usług oraz dostarczania towarów i usług (Dz.U. L 373 z 21.12.2004, s. 37).

([18]) Zob. zwłaszcza Kidron, Evans, Afia (2018 r.), „*Disrupted Childhood – The Cost of Persuasive Design*" („Zaburzone dzieciństwo: koszt perswazyjnego projektowania"), 5Rights Foundation.

([19]) Sprawozdanie grupy wysokiego szczebla w sprawie wpływu transformacji cyfrowej na rynki pracy UE, 2019 r.

([20]) Dyrektywa Rady z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz.U. L 210 z 7.8.1985, s. 29).