Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Biała księga w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i zaufania”

(COM(2020) 65 final)

(2020/C 364/12)

Sprawozdawca: **Catelijne MULLER**

Wniosek o konsultację	Komisja, 9.3.2020
Podstawa prawna	Art. 304 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Jednolitego Rynku, Produkcji i Konsumpcji
Data przyjęcia przez sekcję	25.6.2020
Data przyjęcia na sesji plenarnej	16.7.2020
Sesja plenarna nr	553
Wynik głosowania	
(za/przeciw/wstrzymało się)	207/0/6

1. **Wnioski i zalecenia**

1.1. EKES wyraża uznanie dla Komisji w związku ze strategią zawartą w białej księdze w sprawie sztucznej inteligencji, mającą na celu promowanie stosowania technologii sztucznej inteligencji (SI) a jednocześnie zapewnienie ich zgodności z europejskimi normami etycznymi, wymogami prawnymi i wartościami społecznymi.

1.2. EKES z zadowoleniem przyjmuje również cel, jakim jest wykorzystanie europejskich atutów na rynkach przemysłowych i branżowych, oraz podkreśla znaczenie zwiększenia **inwestycji, infrastruktury, innowacji i umiejętności**, aby umożliwić przedsiębiorstwom, w tym MŚP, i społeczeństwu ogółem wykorzystanie szans oferowanych przez SI. Należy wspierać innowacje w dziedzinie SI w celu maksymalizacji korzyści płynących z systemów sztucznej inteligencji, a jednocześnie zapobiegać zagrożeniom i je minimalizować.

1.3. Uważa jednak, że skoncentrowanie się wyłącznie na sztucznej inteligencji opartej na danych jest zbyt wąskie, aby UE mogła stać się prawdziwym liderem w dziedzinie nowatorskiej, godnej zaufania i konkurencyjnej sztucznej inteligencji. **EKES wzywa Komisję do propagowania również nowej generacji systemów SI, które są oparte na wiedzy i rozumowaniu, a także promują wartości i zasady ludzkie**.

1.4. EKES apeluje do Komisji o: (i) **wspieranie multidyscyplinarnego charakteru badań naukowych** poprzez angażowanie innych dyscyplin, takich jak prawo, etyka, filozofia, psychologia, nauki o pracy, nauki humanistyczne, ekonomia itp.; (ii) **zaangażowanie odpowiednich zainteresowanych stron** (związków zawodowych, organizacji zawodowych, biznesowych i konsumenckich, organizacji pozarządowych) w debatę na temat sztucznej inteligencji oraz jako równorzędnych partnerów w projektach badawczych i innych projektach finansowanych przez UE, takich jak partnerstwo publiczno-prywatne w zakresie SI, dialogi sektorowe oraz program służący wprowadzeniu sztucznej inteligencji w sektorze publicznym i sztandarowe centrum; oraz (iii) dalsze **edukowanie i informowanie ogółu społeczeństwa** w zakresie możliwości i wyzwań związanych ze sztuczną inteligencją.

1.5. EKES nalega, by Komisja bardziej szczegółowo rozważyła **wpływ sztucznej inteligencji na pełne spektrum podstawowych praw i wolności**, w tym m.in. – ale nie tylko – prawo do sprawiedliwego procesu sądowego, do uczciwych i otwartych wyborów oraz do zgromadzeń i demonstracji, a także na prawo do niedyskryminacji.

1.6. Komitet nadal **jest przeciwny wprowadzeniu jakichkolwiek form osobowości prawnej w odniesieniu do sztucznej inteligencji**. Osłabiłoby to zapobiegawczy efekt naprawczy odpowiedzialności prawnej i stworzyłoby poważne ryzyko wystąpienia pokusy nadużycia zarówno w zakresie rozwoju, jak i wykorzystania sztucznej inteligencji.

1.7. EKES postuluje przyjęcie **stałego i systematycznego podejścia społeczno-technicznego** uwzględniającego technologię ze wszystkich punktów widzenia i w świetle różnych kryteriów, zamiast jednorazowych (lub nawet regularnie powtarzanych) wcześniejszych ocen zgodności w zakresie sztucznej inteligencji wysokiego ryzyka.

1.8. EKES ostrzega, że wymóg dotyczący sektora „wysokiego ryzyka" mógłby wykluczyć wiele zastosowań i aplikacji związanych ze sztuczną inteligencją, które są nieodłącznie związane z wysokim ryzykiem, a ponadto identyfikację biometryczną i sztuczną inteligencję stosowaną przy doborze personelu. EKES zaleca Komisji sporządzenie wykazu **wspólnych cech aplikacji lub zastosowań SI, które są uważane za wysoce ryzykowne same w sobie,** niezależnie od sektora.

1.9. EKES stanowczo nalega, by stosowanie systemu identyfikacji biometrycznej było dozwolone wyłącznie: (i) gdy istnieje naukowo udowodniony skutek; (ii) w kontrolowanych środowiskach; i (iii) na ściśle określonych warunkach. **Należy zakazać powszechnego stosowania SI na potrzeby identyfikacji biometrycznej do celów nadzoru lub śledzenia, oceny lub kategoryzacji ludzi lub ludzkich zachowań czy emocji**.

1.10. EKES opowiada się za **wczesnym i ścisłym zaangażowaniem partnerów społecznych** podczas wprowadzania systemów SI w miejscach pracy, zgodnie z obowiązującymi przepisami i praktykami, w celu zapewnienia użyteczności systemów i ich zgodności z prawami pracowników i warunkami pracy.

1.11. EKES opowiada się również za wczesnym i ścisłym zaangażowaniem podczas wprowadzania systemów SI tych pracowników, którzy ostatecznie będą wykorzystywać w pracy system SI, a także tych, którzy posiadają wiedzę fachową w dziedzinie prawa, etyki i nauk humanistycznych, tak aby zapewnić dostosowanie tych systemów do wymogów prawnych i etycznych i potrzeb pracowników oraz umożliwić pracownikom zachowanie autonomii w pracy i stworzyć takie systemy SI, które podnoszą umiejętności pracowników i ich zadowolenie z pracy.

1.12. **Techniki i sposoby podejścia w zakresie sztucznej inteligencji stosowane do zwalczania pandemii COVID-19 powinny być solidne, skuteczne, przejrzyste i możliwe do wyjaśnienia. Powinny one również stać na straży praw człowieka, zasad etycznych i obowiązującego prawodawstwa, a także być uczciwe, sprzyjające włączeniu społecznemu i dobrowolne**.

1.13. EKES wzywa Komisję do odegrania wiodącej roli w celu zapewnienia lepszej koordynacji w całej Europie stosowanych rozwiązań opartych na SI i sposobów podejścia wykorzystywanych do zwalczania pandemii COVID-19.

2. **Biała księga UE w sprawie sztucznej inteligencji**

2.1. EKES z zadowoleniem przyjmuje fakt, że Komisja Europejska bierze pod uwagę wiele zaleceń zawartych we wcześniejszych opiniach Komitetu i grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji, zachęcając do stosowania technologii SI przy jednoczesnym zapewnieniu ich zgodności z normami etycznymi, wymogami prawnymi i wartościami społecznymi UE, w oparciu o to, co sama Komisja nazywa „ekosystemem doskonałości i zaufania".

2.2. Komitet z zadowoleniem przyjmuje propozycje skierowane do przedsiębiorstw, w tym MŚP, i do ogółu społeczeństwa, co pozwala czerpać korzyści z rozwoju i wykorzystania sztucznej inteligencji. Podkreśla także znaczenie zwiększenia inwestycji, infrastruktury, innowacji i umiejętności w celu poprawy konkurencyjności UE w wymiarze globalnym.

Podejście oparte na nadzorczej roli człowieka

2.3. Biała księga ma jednak również nieco „fatalistyczny" wydźwięk i zawiera sugestie, że sztuczna inteligencja „opanowuje nas", nie pozostawiając nam innego wyboru niż uregulowanie jej stosowania. EKES jest w pełni przekonany co do zobowiązania UE do zadbania o to, by Europa akceptowała wyłącznie godną zaufania sztuczną inteligencję, i w związku z tym sądzi, że należy podjąć tu odważniejsze kroki. Komitet wzywa więc Komisję, by opcja niezaakceptowania określonego rodzaju SI (i jej wykorzystania) pozostała zawsze dostępna. Właśnie takie podejście EKES określał mianem „**zasady ludzkiej kontroli**" w odniesieniu do sztucznej inteligencji i musimy je pielęgnować.

Wykorzystanie sztucznej inteligencji w Europie – definicja przyszłościowa

2.4. Robocza definicja SI zawarta w białej księdze określa ją jako „zbiór technologii łączących dane, algorytmy i moc obliczeniową". W dalszej części tekstu **dane** i **algorytmy** definiuje się jako główne elementy sztucznej inteligencji. Jednakże definicja ta obejmowałaby każdy segment oprogramowania, które kiedykolwiek zostało opracowane, a nie tylko SI. Nadal nie istnieje powszechnie obowiązująca definicja sztucznej inteligencji, która jest określeniem ogólnym dla szeregu aplikacji komputerowych.

2.5. **Skoncentrowanie się w białej księdze wyłącznie na sztucznej inteligencji opartej na danych jest zbyt wąskie, aby UE mogła stać się prawdziwym liderem w dziedzinie nowatorskiej, godnej zaufania i konkurencyjnej sztucznej inteligencji**. Biała księga wyłącza wiele obiecujących systemów sztucznej inteligencji z rozważań, a co za tym idzie, z zarządzania i regulacji. EKES wzywa Komisję do promowania również nowej generacji systemów SI, które łączą podejścia oparte na danych z **podejściami opartymi na wiedzy i rozumowaniu**, czyli tzw. systemów hybrydowych. W białej księdze uznaje się potrzebę stworzenia systemów hybrydowych do celów **wytłumaczalności**, ale zalety systemów hybrydowych wykraczają poza wytłumaczalność: mogą one przyspieszyć i/lub spowolnić proces uczenia się oraz zatwierdzać i weryfikować model uczenia maszynowego.

2.6. Biała księga koncentruje się jedynie na stronniczości w odniesieniu do danych, ale nie we wszystkich przypadkach stronniczość wynika z niskiej jakości lub ograniczonej liczby danych. **Konstrukcja każdego artefaktu jest sama w sobie kumulacją stronniczych wyborów**, począwszy od rozważanych nakładów, a skończywszy na celach wyznaczonych do optymalizacji. Wszystkie te wybory są w taki czy inny sposób napędzane przez wrodzoną stronniczość osoby (osób), która (e) ich dokonuje(ą).

2.7. Przede wszystkim jednak systemy SI są czymś więcej niż tylko sumą komponentów oprogramowania. **Obejmują one również otaczający je system społeczno-techniczny**. Refleksja nad zarządzaniem i regulacją w zakresie SI powinna również koncentrować się na otaczającym ją kontekście struktur społecznych: organizacjach, przedsiębiorstwach, różnych zawodach, osobach i instytucjach, które tworzą, rozwijają, wprowadzają, stosują i kontrolują SI, a także na podmiotach, na które SI wywiera wpływ, takich jak obywatele i ich związek z rządami, firmy, konsumenci, pracownicy, a nawet całe społeczeństwo.

2.8. Należy również zauważyć, że **definicje prawne (do celów zarządzania i regulacji) różnią się od definicji czysto naukowych**, ponieważ konieczne jest spełnienie szeregu różnych wymogów, takich jak inkluzywność, precyzyjność, trwałość, kompletność i wykonalność. Niektóre z nich są wymogami prawnie wiążącymi, a inne są uważane za dobre praktyki regulacyjne.

Połączenie wszystkich sił

2.9. EKES z zadowoleniem przyjmuje wysiłki na rzecz rozwiązania problemu rozdrobnienia SI w Europie poprzez skupienie naukowców zajmujących się sztuczną inteligencją i skoncentrowanie się na MŚP oraz partnerstwie z sektorem prywatnym i publicznym. Ponadto Komitet zalecałby: (i) wspieranie multidyscyplinarnego charakteru badań naukowych poprzez angażowanie innych dyscyplin, takich jak prawo, etyka, filozofia, psychologia, nauki o pracy, nauki humanistyczne, ekonomia itp.; (ii) zaangażowanie odpowiednich zainteresowanych stron (związków zawodowych, organizacji biznesowych i konsumenckich, organizacji pozarządowych) w debatę na temat sztucznej inteligencji oraz jako równorzędnych partnerów w projektach badawczych i innych projektach finansowanych przez UE, takich jak partnerstwo publiczno-prywatne w zakresie SI, dialog sektorowy oraz program służący wprowadzeniu sztucznej inteligencji w sektorze publicznym i sztandarowe centrum; oraz (iii) dalsze edukowanie ogółu społeczeństwa w zakresie możliwości i wyzwań związanych ze sztuczną inteligencją.

SI a prawo

2.10. W białej księdze uznaje się fakt, że **sztuczna inteligencja nie funkcjonuje w świecie, w którym nie ma prawa**. EKES ze szczególnym zadowoleniem przyjmuje nacisk, jaki kładzie się na skutki sztucznej inteligencji dla praw podstawowych, i zaleca, aby Komisja bardziej szczegółowo rozważyła wpływ sztucznej inteligencji na szeroki zestaw podstawowych praw i wolności, takich jak wolność słowa i wypowiedzi, prawo do poszanowania życia prywatnego (które wykracza poza ochronę danych osobowych), do sprawiedliwego procesu sądowego, do uczciwych i otwartych wyborów, do zgromadzeń i demonstracji oraz do niedyskryminacji.

2.11. EKES z zadowoleniem przyjmuje jasne stanowisko przyjęte w białej księdze w sprawie stosowania istniejących systemów odpowiedzialności w odniesieniu do sztucznej inteligencji i wysiłki na rzecz wykorzystania tych systemów w celu rozwiązania problemu nowych zagrożeń, jakie może stworzyć sztuczna inteligencja, usunięcia luk w zakresie egzekwowania przepisów tam, gdzie trudno jest ustalić, który podmiot gospodarczy jest rzeczywiście odpowiedzialny, oraz dostosowania systemów do zmieniającej się funkcjonalności systemów sztucznej inteligencji.

2.12. Komisja powinna również uznać, że sztuczna inteligencja nie zna granic i że wysiłki nie mogą i nie powinny ograniczać się do samej Europy. W celu ustanowienia wspólnych międzynarodowych ram prawnych należy osiągnąć ogólny konsensus na całym świecie w oparciu o dyskusje i badania przeprowadzone przez ekspertów prawnych.

2.13. Tak czy inaczej EKES nadal jest **stanowczo przeciwny wprowadzeniu jakichkolwiek form osobowości prawnej w odniesieniu do sztucznej inteligencji**. Osłabiłoby to zapobiegawczy efekt naprawczy odpowiedzialności prawnej i stworzyłoby poważne ryzyko wystąpienia pokusy nadużycia zarówno w zakresie rozwoju, jak i wykorzystania sztucznej inteligencji.

Regulacja SI wysokiego ryzyka

2.14. EKES z zadowoleniem przyjmuje podejście oparte na analizie ryzyka w odniesieniu do kontrolowania wpływu sztucznej inteligencji. Komisja zapowiada ramy regulacyjne dotyczące „sztucznej inteligencji wysokiego ryzyka", która musiałaby spełniać wymogi dotyczące solidności, dokładności, odtwarzalności, przejrzystości, nadzoru ze strony człowieka i zarządzania danymi. Zgodnie z białą księgą na sztuczną inteligencję wysokiego ryzyka składają się dwa elementy: (i) sektor wysokiego ryzyka oraz (ii) zastosowanie SI wysokiego ryzyka. W białej księdze dodano dwa przykłady zastosowań i aplikacji w dziedzinie sztucznej inteligencji, które są uważane za wysoce ryzykowne z natury rzeczy, tj. niezależnie od sektora. Do zastosowań o wysokim poziomie ryzyka zakwalifikowano w niej również identyfikację biometryczną. Wyczerpujący wykaz sektorów wysokiego ryzyka (który jest poddawany okresowym przeglądom) obejmuje obecnie następujące sektory potencjalnie wysokiego ryzyka: opieka zdrowotna, transport, energetyka i elementy sektora publicznego.

2.15. Drugie kryterium, tj. stosowanie sztucznej inteligencji związane z zagrożeniami, jest mniej rygorystyczne, co sugeruje, że można uwzględnić różne poziomy ryzyka. EKES proponuje, by do obszarów oddziaływania dodać społeczeństwo i środowisko naturalne.

2.16. Zgodnie z logiką białej księgi, stosowanie sztucznej inteligencji **wysokiego ryzyka** w sektorze **niskiego ryzyka** nie będzie co do zasady podlegać ramom regulacyjnym. Komitet zwraca uwagę, że niepożądane niekorzystne skutki sztucznej inteligencji wysokiego ryzyka w sektorze niskiego ryzyka mogłyby spowodować wyłączenie niektórych zastosowań lub aplikacji SI, tworząc „okno" pozwalające na obejście przepisów: należy pomyśleć o ukierunkowanej reklamie (sektor niskiego ryzyka), co do której wykazano, że może prowadzić do segregacji, dyskryminacji i podziałów, np. podczas wyborów lub dzięki spersonalizowanym cenom (zastosowanie lub efekt wysokiego ryzyka). **EKES zaleca opracowanie wykazu wspólnych cech aplikacji lub zastosowań w dziedzinie SI, które są uważane za wysoce ryzykowne „jako takie"** niezależnie od sektora, w którym się je wykorzystuje.

2.17. Chociaż Komitet uznaje potrzebę badania zgodności sztucznej inteligencji, obawia się, że jednorazowa (lub nawet regularnie powtarzana) **wcześniejsza ocena zgodności** nie wystarczy, aby zagwarantować godny zaufania i ukierunkowany na człowieka rozwój, wprowadzanie i wykorzystywanie SI w sposób zrównoważony. **Godna zaufania sztuczna inteligencja wymaga ciągłego, systematycznego podejścia społeczno-technicznego**, uwzględniającego technologię ze wszystkich perspektyw i w świetle różnych kryteriów. Z punktu widzenia kształtowania polityki wymaga to multidyscyplinarnego podejścia, w ramach którego decydenci polityczni, naukowcy z różnych dziedzin, partnerzy społeczni, organizacje zawodowe, specjaliści, przedsiębiorstwa i organizacje pozarządowe stale współpracują ze sobą. Zwłaszcza w odniesieniu do usług użyteczności publicznej związanych ze zdrowiem, bezpieczeństwem i dobrostanem ludzi i opartych na zaufaniu należy zagwarantować, że systemy SI zostaną dostosowane do wymogów praktycznych i nie przejmą odpowiedzialności człowieka.

Identyfikacja biometryczna

2.18. EKES z zadowoleniem przyjmuje wezwanie Komisji do rozpoczęcia publicznej debaty na temat zastosowania SI do celów identyfikacji biometrycznej. Identyfikacja biometryczna mikroekspresji, chodu, (tonu) głosu, tętna, temperatury itd. jest już wykorzystywana do oceny lub nawet przewidywania naszego zachowania, stanu psychicznego i emocji, w tym podczas procesów rekrutacji. Należy bardzo wyraźnie stwierdzić, że **nie istnieją żadne solidne dowody naukowe sugerujące, że wewnętrzne emocje lub stan psychiczny danej osoby można dokładnie „odczytać" z jej mimiki twarzy, chodu, tętna, tonu głosu lub temperatury, ani tym bardziej, że można w ten sposób przewidzieć przyszłe zachowanie danej osoby**.

2.19. **Trzeba również zauważyć, że ogólne rozporządzenie o ochronie danych (RODO) ogranicza jedynie w pewnym stopniu przetwarzanie danych biometrycznych**. W RODO dane biometryczne zdefiniowano jako „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej". Wiele technologii identyfikacji biometrycznej nie ma jednak na celu jednoznacznej identyfikacji osoby, lecz jedynie ocenę zachowania lub emocji danej osoby. Zastosowania te mogą nie wchodzić w zakres definicji (przetwarzania) danych biometrycznych na mocy ogólnego rozporządzenia o ochronie danych.

2.20. Zastosowanie SI do celów identyfikacji biometrycznej ma również wpływ na nasze szersze prawo do poszanowania życia prywatnego, tożsamości, niezależności i integralności psychicznej poprzez stworzenie sytuacji, w której jesteśmy (stale) obserwowani, śledzeni i identyfikowani. **Może to mieć psychologiczny „efekt odstraszający", zmuszając obywateli do dostosowania zachowania do określonej normy**. Jest to ingerencja w nasze podstawowe prawo do prywatności (integralności moralnej i psychicznej). Ponadto zastosowanie SI do celów identyfikacji biometrycznej może mieć wpływ na inne podstawowe prawa i wolności, takie jak wolność zgromadzeń i prawo do niedyskryminacji.

2.21. EKES zaleca, by stosowanie identyfikacji biometrycznej **było dozwolone wyłącznie wtedy, gdy istnieje naukowo udowodniony skutek, w kontrolowanych środowiskach i na ściśle określonych warunkach**. Nie należy zezwalać na powszechne stosowanie SI do celów identyfikacji biometrycznej do prowadzenia nadzoru lub śledzenia, oceny lub kategoryzacji ludzi lub ludzkich zachowań lub emocji.

Wpływ SI na zatrudnienie i umiejętności

2.22. EKES zauważa, że w białej księdze brakuje strategii dotyczącej wpływu sztucznej inteligencji na pracę, podczas gdy był to wyraźny element europejskiej strategii na rzecz sztucznej inteligencji z 2018 r.

2.23. Komitet opowiada się za **wczesnym i ścisłym zaangażowaniem wszelkiego rodzaju pracowników i usługodawców, w tym freelancerów, osób samozatrudnionych i pracowników dorywczych** – nie tylko tych, którzy projektują lub rozwijają sztuczną inteligencję, ale również tych, którzy nabywają i wdrażają systemy sztucznej inteligencji, pracują na nich lub doświadczają ich wpływu. **Dialog społeczny musi mieć miejsce przed** wprowadzeniem technologii sztucznej inteligencji w miejscu pracy zgodnie z obowiązującymi przepisami i praktykami. Dostęp do danych dotyczących pracowników i zarządzanie nimi w miejscu pracy powinny opierać się na zasadach i przepisach wynegocjowanych przez partnerów społecznych.

2.24. EKES pragnie zwrócić szczególną uwagę na **sztuczną inteligencję wykorzystywaną w procesach rekrutacji, zwalniania, weryfikacji i oceny pracowników**. W białej księdze wspomina się o sztucznej inteligencji stosowanej w procesie rekrutacji jako przykładzie zastosowania wysokiego ryzyka, które podlegałoby regulacji niezależnie od sektora. EKES zaleca rozszerzenie tego obszaru zastosowania o sztuczną inteligencję stosowaną w procesach zwalniania, weryfikacji i oceny pracowników, a także zbadanie wspólnych cech zastosowań SI, które wiązałyby się z wysokim ryzykiem użycia w miejscu pracy niezależnie od sektora. Zastosowania SI, które nie mają podstaw naukowych, takie jak wykrywanie emocji poprzez identyfikację biometryczną, nie powinny być dozwolone w środowisku pracy.

2.25. Aby umożliwić ludziom dostosowywanie się do szybkich przemian zachodzących na polu sztucznej inteligencji, niezbędne jest utrzymanie lub zdobycie umiejętności cyfrowych. Jednak powinna także istnieć możliwość **ukierunkowania** strategii politycznych i środków finansowych **na kształcenie i rozwój umiejętności** w dziedzinach, w których systemy sztucznej inteligencji nie stwarzają zagrożenia (np. zadania, w przypadku których kluczowe znaczenie ma ludzka interakcja, takie jak usługi użyteczności publicznej związane ze zdrowiem, bezpieczeństwem i dobrostanem ludzi i oparte na zaufaniu, w przypadku których ludzie i maszyny współpracują ze sobą, lub zadania, które chcielibyśmy nadal powierzać człowiekowi).

3. **SI a koronawirus**

3.1. Sztuczna inteligencja może przyczynić się do lepszego zrozumienia koronawirusa i COVID-19, a także do ochrony ludzi przed narażeniem na niego, do znalezienia szczepionki i zbadania możliwości leczenia. Ważne jest jednak, aby jasno i otwarcie rozróżnić, do czego sztuczna inteligencja jest zdolna a do czego nie.

3.2. **Wytrzymałość i skuteczność**: wykorzystanie sztucznej inteligencji opartej na danych w celu prognozowania rozprzestrzeniania się koronawirusa jest potencjalnie problematyczne, ponieważ dane dotyczące koronawirusa są zbyt skąpe, aby SI pozwoliła uzyskać wiarygodne wyniki. Ponadto nieliczne dane, które stały się dostępne, są niepełne i stronnicze. Ich wykorzystywanie do uczenia maszynowego może prowadzić do wielu wyników fałszywie ujemnych i fałszywie dodatnich.

3.3. Kluczowe znaczenie mają **przejrzystość** stosowanych danych i modeli oraz **wytłumaczalność** wyników. W tej chwili świat nie może sobie pozwolić na podejmowanie decyzji w oparciu o „czarne skrzynki".

3.4. Przy wykorzystywaniu SI do zwalczania tej pandemii **poszanowanie praw człowieka, zasad etycznych i istniejącego prawodawstwa** jest ważniejsze niż kiedykolwiek wcześniej. W szczególności gdy narzędzia SI potencjalnie naruszają prawa człowieka, musi istnieć uzasadniony interes w ich stosowaniu, a takie stosowanie musi być absolutnie niezbędne, proporcjonalne i przede wszystkim ograniczone w czasie.

3.5. Ponadto musimy zapewnić **uczciwość i włączenie społeczne**. Opracowywane systemy sztucznej inteligencji na potrzeby zwalczania pandemii powinny być wolne od uprzedzeń i niedyskryminujące. Co więcej, powinny być one dostępne dla wszystkich oraz uwzględniać różnice społeczne i kulturowe między poszczególnymi krajami dotkniętymi pandemią.

Aplikacje do śledzenia i wyszukiwania kontaktów oraz aplikacje do monitorowania stanu zdrowia

3.6. Zdaniem wirusologów i epidemiologów otwarcie społeczeństwa i gospodarki po wprowadzeniu środków izolacji wymaga skutecznego śledzenia, ustalania kontaktów zakaźnych, monitorowania i ochrony zdrowia ludzi. Obecnie opracowuje się wiele **aplikacji** mających na celu śledzenie, ustalanie kontaktów zakaźnych i przeprowadzanie kontroli zdrowia, czym zazwyczaj (w przeszłości) zajmowali się odpowiedni specjaliści. Na całym świecie wiele rządów pokłada ogromne zaufanie w aplikacjach do śledzenia i wyszukiwania kontaktów jako narzędziach umożliwiających ponowne otwarcie się społeczeństw.

3.7. Wprowadzenie tego rodzaju aplikacji jest bardzo radykalnym krokiem. Dlatego też ważne jest, aby przed podjęciem decyzji o ich wykorzystaniu krytycznie zbadać **przydatność, konieczność i skuteczność** tych aplikacji, a także ich skutki społeczne i prawne. Nadal musi istnieć możliwość ich niestosowania, a mniej inwazyjne rozwiązania powinny być traktowane priorytetowo.

3.8. **Skuteczność i niezawodność** aplikacji do śledzenia i wyszukiwania kontaktów jest niezwykle istotna, ponieważ nieskuteczność i zawodność mogą prowadzić do wielu fałszywie dodatnich i fałszywie ujemnych wyników, fałszywego poczucia bezpieczeństwa, a tym samym większego ryzyka zarażenia. Wstępne symulacje naukowe budzą poważne wątpliwości co do tego, czy aplikacja umożliwiająca śledzenie będzie miała jakikolwiek pozytywny wpływ na powstrzymanie rozprzestrzeniania się wirusa, nawet jeśli 80 % lub 90 % populacji będzie jej używać. Ponadto aplikacja nie może rejestrować szczególnych okoliczności, takich jak obecność pleksiglasu i okien czy noszenie środków ochrony osobistej.

3.9. Co więcej, **aplikacje te pociągają za sobą (częściowe) zawieszenie różnego rodzaju praw człowieka i swobód**, ponieważ wpływają na wolność zrzeszania się, prawo do bezpieczeństwa, prawo do niedyskryminacji i prawo do prywatności.

3.10. Choć prywatność jest bardzo ważna, znaczy ona o wiele więcej niż nasze dane osobowe i anonimowość. Prywatność dotyczy również prawa do tego, by nie być śledzonym, namierzanym i poddawanym nadzorowi. Zostało naukowo udowodnione, że ludzie, którzy wiedzą, że ich ruchy są śledzone, zaczynają zachowywać się w sposób odmienny. Zdaniem Europejskiego Trybunału Praw Człowieka ten „efekt odstraszający" stanowi naruszenie naszej prywatności. W debacie na temat sztucznej inteligencji należy stosować tę samą szeroką koncepcję prywatności.

3.11. Zachodzi ryzyko, że gromadzone dane (obecnie lub w przyszłości) zostaną wykorzystane nie tylko do zwalczania obecnej pandemii, ale także do profilowania, kategoryzowania i oceny poszczególnych osób w różnych celach. W bardziej odległej przyszłości można nawet wyobrazić sobie, że **„rozrost funkcji"** może prowadzić do niepożądanego rodzaju profilowania w zakresie kontroli i nadzoru, akceptacji ubezpieczeń lub świadczeń socjalnych, zatrudnienia lub zwolnienia itp. Dane zebrane za pomocą takich aplikacji nie mogą być zatem w żadnym wypadku wykorzystywane do profilowania, oceny ryzyka, klasyfikowania lub prognozowania.

3.12. Ponadto **każde rozwiązanie polegające na sztucznej inteligencji stosowane w tych nadzwyczajnych okolicznościach, nawet z najlepszymi intencjami, stworzy precedens**, niezależnie od tego, czy nam się to podoba, czy też nie. Poprzednie kryzysy pokazały, że mimo wszelkich dobrych intencji tego rodzaju środki w praktyce nigdy nie znikną.

3.13. Dlatego też stosowanie sztucznej inteligencji podczas obecnej pandemii powinno być zawsze mierzone i analizowane z uwzględnieniem różnych czynników, takich jak: (i) Czy jest ono skuteczne i godne zaufania? (ii) Czy istnieją mniej inwazyjne rozwiązania? (iii) Czy płynące stąd korzyści przeważają nad problemami społecznymi, etycznymi i związanymi z prawami podstawowymi? (iv) Czy można osiągnąć kompromis między sprzecznymi ze sobą podstawowymi prawami i swobodami? Ponadto tego rodzaju systemy **nie mogą być wprowadzane w formie jakiegokolwiek zobowiązania lub przymusu**.

3.14. EKES wzywa decydentów politycznych, by **nie akceptowali zbyt łatwo mody na rozwiązania techniczne**. Biorąc pod uwagę powagę sytuacji, zalecamy, aby aplikacje związane z projektami mającymi na celu wspomaganie opanowania pandemii były oparte na solidnych badaniach w dziedzinie nauk epidemiologicznych, socjologii, psychologii, prawa, etyki i nauk o systemach. Przed podjęciem decyzji o zastosowaniu tych systemów należy przeprowadzić analizę skuteczności, konieczności i czułości oraz symulacje.

Bruksela, dnia 16 lipca 2020 r.

Luca JAHIER
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego