

Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Zwalczanie dezinformacji w internecie: podejście europejskie”

[COM(2018) 236 final]

(2018/C 440/32)

Sprawozdawca: **Martin SIECKER**

Wniosek o konsultację	Komisja Europejska, 18.6.2018
Podstawa prawna	Art. 304 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego
Data przyjęcia przez sekcję	6.9.2018
Data przyjęcia na sesji plenarnej	19.9.2018
Sesja plenarna nr	537
Wynik głosowania	121/16/34
(za / przeciw / wstrzymało się)	

1. Wnioski i zalecenia

1.1. Wolność informacji i wypowiedzi to w UE nienaruszalne prawo, jednak można ją też wykorzystywać do obalania zasad Unii w celu uniemożliwienia debaty i krytycznego myślenia – wykorzystywać nie jako narzędzie informowania lub przekonywania, lecz jako oręż. Dezinformację stosuje się jako skrajną formę nadużycia mediów, która zmierza do wywarcia wpływu na procesy społeczne i polityczne i zyskuje szczególną siłę, kiedy jest sponsorowana przez rządy i wykorzystywana w stosunkach międzynarodowych. Obecnie jej jaskrawymi przypadkami są, pośród wielu innych, rosyjska kampania dezinformacyjna wspierana przez państwo, kampania na rzecz brexitu, którą da się nazwać tylko frontalnym atakiem na UE, i ingerencja w wybory w USA. Wszystkie te działania destabilizacyjne budzą poważne obawy w europejskim społeczeństwie obywatelskim.

1.2. Wykorzystuje się dzisiaj różnorakie narzędzia i metody, aby podważać wartości europejskie i działania zewnętrzne UE, a także wzmacniać i rozbudzać postawy separatystyczne i nacjonalistyczne, manipulować opinią publiczną i bezpośrednio ingerować w politykę wewnętrzną suwerennych państw i UE jako całości. Ponadto daje się zaobserwować coraz większy wpływ ofensywnych zdolności cybernetycznych i intensywniejsze wykorzystywanie technologii do produkcji broni z myślą o osiągnięciu celów politycznych. Wpływ takich działań często pozostaje niedoceniony⁽¹⁾.

1.3. EKES zgadza się z Komisją, która apeluje o większą odpowiedzialność ze strony platform mediów społecznościowych. Pomimo ukazania się w ostatnich latach kilku badań i dokumentów programowych autorstwa europejskich specjalistów, komunikat nie przewiduje jednak żadnych obowiązkowych praktycznych kroków w tym kierunku.

1.4. Na podstawie dostępnych opracowań UE powinna zapewnić i kontynuować badania w zakresie wpływu dezinformacji w Europie, również poprzez uwzględnienie w przyszłych sondażach Eurobarometru monitorowania odporności Europejczyków na dezinformację. Sondaże te powinny obejmować nie tylko ogólne dane dotyczące fałszywych informacji, lecz także pozwolić określić faktyczną odporność Europejczyków na dezinformację. Komisja nie traktuje sprawy jako naglącej i brakuje jej ambicji, dlatego nie odnosi się do zasadniczych kwestii takich jak systemy wsparcia dla tradycyjnych mediów w celu zagwarantowania podstawowego prawa obywateli do wysokiej jakości wiarygodnych informacji, zbadanie możliwości ustanowienia partnerstw publiczno-prywatnych w celu tworzenia płatnych platform internetowych oferujących bezpieczne i przystępne cenowo usługi online, przestudiowanie możliwości zapewnienia większej przejrzystości algorytmów leżących u podstaw tych systemów internetowych oraz zapewnienia większego nadzoru nad tymi algorytmami, a także zanalizowanie sposobności rozbicia monopolu w celu przywrócenia równych warunków działania dla uczciwej konkurencji, aby zapobiec stopniowemu korumpowaniu społeczeństwa.

⁽¹⁾ Raport informacyjny REX/432 „Wykorzystywanie mediów do wpływania na procesy społeczne i polityczne w UE i wschodnich państwach sąsiednich”.

1.5. EKES wyraża ubolewanie w związku z tym, że zarówno w komunikacie, jak i w sprawozdaniu grupy ekspertów wysokiego szczebla nie wspomina się o Rosji jako głównym źródle wrogiej dezinformacji skierowanej przeciwko UE. A przecież pierwszym krokiem do rozwiązania każdego problemu jest przyznanie, że takowy istnieje.

1.6. Na podstawie rezolucji Parlamentu Europejskiego z dnia 15 czerwca 2017 r. w sprawie platform internetowych i jednolitego rynku cyfrowego⁽²⁾ Komisja odniosła się do apeli EKES-u o należyte egzekwowanie istniejących przepisów prawnych dotyczących platform internetowych. Ponadto EKES zachęca Komisję do zakończenia dyskusji nad systemem odpowiedzialności prawnej dla platform internetowych i do wdrożenia regulacji, które konkretnie odnoszą się do definicji i charakteru tychże platform. Platformy internetowe i sieci społecznościowe powinny zobowiązać się do przestrzegania tych zasad w celu zapewnienia przejrzystości dzięki wyjaśnieniu, w jaki sposób algorytmy dokonują wyboru prezentowanych wiadomości. Należy także zachęcać te podmioty do przedsięwzięcia skutecznych środków z myślą o poprawie widoczności wiarygodnych, rzetelnych informacji i ułatwieniu użytkownikom dostępu do nich.

1.7. Jednym z problemów związanych z dezinformacją jest brak możliwości sprawdzenia tożsamości źródeł rozpowszechniających dezinformację w internecie. Działanie w cyberprzestrzeni pod fałszywą tożsamością jest zbyt łatwe – i ogólnie właśnie tak postępują osoby, które działają w sieci w złych zamiarach. Komisja przedstawia kilka propozycji, które zostały określone we wspólnym komunikacie na temat bezpieczeństwa cybernetycznego opublikowanym we wrześniu 2017 r. Problem polega na tym, że propozycje te nie mają wiążącego charakteru. Jeśli rzeczywiście chcemy poczynić postępy w walce z dezinformacją, możemy potrzebować ostrzejszych środków dotyczących identyfikacji w przypadku osób aktywnie działających w internecie. W końcu tak właśnie funkcjonują wysokiej jakości media informacyjne, zgodnie z kodeksem z Bordeaux z 1954 r. uchwalonym przez Międzynarodową Federację Dziennikarzy, który określa bardzo jasne i ścisłe zasady pracy ze źródłami. Nazwy i adresy źródeł zawsze muszą być znane personelowi redakcyjnemu.

1.8. EKES zgadza się z Komisją co do potrzeby ścisłej współpracy społeczności weryfikującej fakty. Podobne sieci już istnieją, w tym jedna działająca w ramach grupy zadaniowej East StratCom. Jednak potrzebują one odpowiedniego finansowania, którego obecnie brakuje. EKES wzywa Komisję oraz państwa członkowskie do pełnego wsparcia wysiłków grupy zadaniowej East StratCom. Powinno to obejmować nie tylko odpowiedni budżet, ale także aktywne zaangażowanie wszystkich państw członkowskich w prace tej grupy – zaangażowanie polegające przede wszystkim na oddelegowaniu ekspertów do grupy zadaniowej East StratCom i tworzeniu punktów kontaktowych. Informacje o stronie internetowej przedstawiającej wyniki pracy tej grupy zadaniowej⁽³⁾ powinny być przekazywane bardziej aktywnie, aby podnieść w UE społeczną świadomość tych zagrożeń.

2. Streszczenie komunikatu Komisji

2.1. Dobrze funkcjonujący, wolny i pluralistyczny ekosystem informacyjny, oparty na wysokich standardach zawodowych, jest niezbędny do prowadzenia zdrowej demokratycznej debaty. Komisja jest czujna na zagrożenia dla naszych otwartych i demokratycznych społeczeństw stwarzane przez dezinformację.

2.2. Komisja zamierza przedstawić kompleksowe podejście, które ma na celu reagowanie na te zagrożenia poprzez promowanie ekosystemów cyfrowych⁽⁴⁾ opartych na przejrzystości i uprzywilejowaniu dostępu do informacji wysokiej jakości, umożliwienie obywatelom skuteczniejszej obrony przed dezinformacją oraz ochronę naszych demokracji i procesów decyzyjnych.

2.3. Komisja wzywa wszystkie zainteresowane podmioty, by dołożyły starań w celu właściwego rozwiązania problemu dezinformacji. Uważa, że proponowane działania, o ile zostaną skutecznie wdrożone, przyczynią się w istotny sposób do zwalczania dezinformacji w internecie.

2.4. Komisja określa trzy główne przyczyny problemu (tworzenie dezinformacji, nagłośnienie w mediach społecznościowych i innych mediach internetowych, rozpowszechnienie przez użytkowników platform internetowych) i przedstawia szereg propozycji rozwiązań w pięciu obszarach polityki:

- stworzenie bardziej przejrzystego, godnego zaufania i odpowiedzialnego ekosystemu internetowego,
- bezpieczne i odporne procesy wyborcze,

⁽²⁾ 2016/2276 (INI).

⁽³⁾ <https://euvsdisinfo.eu>.

⁽⁴⁾ Komisja używa w swoim dokumencie słowa „ekosystemy”. W tym kontekście właściwsze byłoby słowo „infrastruktura”.

- wspieranie edukacji i umiejętności korzystania z mediów,
- wsparcie dla wysokiej jakości dziennikarstwa jako istotnego elementu demokratycznego społeczeństwa,
- zwalczanie wewnętrznych i zewnętrznych zagrożeń wynikających z dezinformacji poprzez komunikację strategiczną.

3. Uwagi ogólne

3.1. Wzrost zorganizowanej dezinformacji za sprawą różnych podmiotów państwowych i niepaństwowych stanowi realne zagrożenie dla demokracji. Destabilizujące siły obejmują rządy państw większych niż jakiekolwiek państwo członkowskie Unii. Jeżeli Unia chce przeciwdziałać temu zagrożeniu, to jest ona odpowiednim partnerem do działania, ponieważ w przeciwieństwie do któregośkolwiek z państw członkowskich posiada masę krytyczną i zasoby, stawiające ją w wyjątkowej pozycji, dzięki której może stworzyć i wdrożyć strategię i politykę służące rozwiązaniu tej złożonej kwestii.

3.2. Prawidłowe funkcjonowanie demokracji zależy od dobrze poinformowanych obywateli, dokonujących świadomych wyborów na podstawie wiarygodnych faktów i zaufanych opinii. Kluczową rolę w tym względzie odgrywa system niezależnych, wiarygodnych i przejrzystych przedsiębiorstw medialnych, w którym specjalna pozycja przypada nadawcom publicznym. Przedsiębiorstwa te zatrudniają dużą liczbę wykwalifikowanych pracowników, którzy zbierają, weryfikują, oceniają, analizują i interpretują nowe źródła w celu zabezpieczenia pewnego poziomu jakości i rzetelności publikowanych informacji.

3.3. Istnieje różnica między fałszywymi informacjami a dezinformacją. Fałszywe informacje są znane w historii od dawna: jest to uniwersalny termin obejmujący plotki, propagandę wojenną, mowę nienawiści, sensacje, kłamstwa, wybiórcze wykorzystywanie faktów itp. Piętnastowieczny wynalazek prasy drukarskiej umożliwił rozpowszechnianie (fałszywych) informacji na większą skalę, a ich zasięg geograficzny zwiększył się jeszcze bardziej po wprowadzeniu znaczka pocztowego w 1840 r. Technologie cyfrowe i internet zniosły ostatnie bariery hamujące nieograniczoną dystrybucję.

3.4. Dezinformację definiuje się jako możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę procesom demokratycznym i wpłynąć na wybory, stanowiąc poważne zagrożenie dla społeczeństwa⁽⁵⁾.

3.5. Łańcuch dezinformacji składa się z wielu różnych podmiotów: tych, którzy ją tworzą, tych, którzy ją konsumują, oraz z platform internetowych odgrywających w całym tym procesie nadrzędną rolę poprzez ułatwianie rozpowszechniania dezinformacji.

Ci, którzy ją tworzą (m.in. rządy, instytucje religijne, koncerty, partie polityczne, organizacje ideologiczne), robią to z różnych przyczyn (aby wpłynąć na opinię publiczną i manipulować nią, potwierdzić swoją domniemaną wyższość, osiągnąć lub zwiększyć zyski, zdobyć władzę, wywołać nienawiść, uzasadnić wykluczenie itp.).

Ci, którzy ją rozpowszechniają (w szczególności platformy internetowe, lecz również media tradycyjne), robią to z różnych przyczyn, w tym w celu uzyskania korzyści finansowych lub dopuszczenia się celowej manipulacji.

Ci, którzy konsumują dezinformację (użytkownicy internetu), często nie są wystarczająco krytycznymi konsumentami, w związku z czym są oni następnie celowo manipulowani przez platformy internetowe. Pośredniczące firmy technologiczne takie jak Twitter, Google i Facebook (aby wymienić tylko kilka z nich) ułatwiają nieograniczone i niekontrolowane udostępnianie treści na platformach internetowych w zamian za gromadzenie danych prywatnych umożliwiających tym platformom osiąganie olbrzymich zysków dzięki mikroukierunkowanej reklamie, dostarczającej indywidualnie dostosowany przekaz reklamowy ściśle określonym grupom docelowym. Niewiedza konsumentów w kwestii samoobrony cyfrowej przyczynia się do pogłębienia tego problemu.

3.6. Przedsiębiorstwa technologiczne, o których mowa, ponoszą wspólną odpowiedzialność, ponieważ odgrywają nadrzędną rolę w tym procesie. Nie postrzegają one siebie jako wydawców, lecz „tylko” jako platformy internetowe, które rozpowszechniają informacje i inne treści stworzone przez uznane media, bez konieczności ponoszenia kosztów tworzenia treści w postaci zatrudniania redakcji. Treści są rozpowszechniane z innych źródeł bez zweryfikowania, oceny, analizy czy interpretacji publikowanych materiałów. „Google to nie »tylko« platforma. Tworzy, kształtuje i fałszuje to, jak widzimy świat” – tak brzmiał jeden z wniosków zawartych w artykule pt. „The great Brexit robbery: how our democracy was hijacked” opublikowanym w *The Guardian*. Przeanalizowano w nim, w jaki sposób „podejrzane globalne działania prowadzone przez [...] różnorodnych zwolenników wystąpienia Zjednoczonego Królestwa z UE wpłynęły na wynik referendum unijnego”. Ponieważ dezinformacja i wiarygodne wiadomości są przedstawiane obok siebie bez wyraźnego

⁽⁵⁾ Komunikat Komisji COM(2018) 236 final.

rozdzielenia, użytkownicy mają trudność z oddzieleniem jednych od drugich. Tak więc firmy technologiczne powinny koncentrować się przede wszystkim na zapewnieniu przejrzystości odnośnie do przepisów i danych. Szczególnie ważna jest przejrzystość powiązań między polityką przychodów z reklam prowadzoną przez platformy a szerzeniem dezinformacji. (W tym kontekście należy ściśle monitorować bieżące negocjacje w sprawie kodeksu postępowania w zakresie dezinformacji, który powinien być zostać opublikowany do końca lipca 2018 r.).

4. Uwagi szczegółowe

4.1. Pomimo różnorodności przekazów, kanałów, narzędzi, poziomów, ambicji i celów taktycznych oraz niezależnie od szybkości, z jaką dezinformacja dostosowuje się do nowych warunków, strategicznym celem kampanii dezinformacyjnych jest podważanie demokracji liberalnej oraz szerzenie i zwiększanie nieufności wobec wiarygodnych źródeł informacji, geopolitycznego kierunku danego kraju i wobec działalności organizacji międzyrządowych. Dezinformację wykorzystuje się do eksploatawania i potęgowania podziałów między różnymi grupami społeczno-gospodarczymi z uwagi na narodowość, rasę, dochody, wiek, wykształcenie i zawód. Oprócz dobrze znanych form takich jak środki przekazu, wykorzystywanie platform internetowych, masowe e-maile itp. istnieją też inne, np. agencje PR, lobbyści, ośrodki analityczne, organizacje pozarządowe, podmioty wpływające na opinię elit, polityka partyjna, społeczności ekspertów, działania kulturalne oraz europejskie ruchy skrajnej prawicy i lewicy, które w zamian otrzymują płatności za pośrednictwem różnorakich „niezależnych” trustów publicznych czy kont bankowych *offshore* itd.

4.2. Rosyjski rząd wykorzystuje w swoich kampaniach dezinformacyjnych szeroki wachlarz narzędzi i instrumentów, jak to stwierdziły już Parlament Europejski⁽⁶⁾, Komisja Europejska⁽⁷⁾ i Rada Europejska⁽⁸⁾. Kampanie te należy traktować niezwykle poważnie. Stanowią one część rosyjskiej doktryny wojskowej i są akceptowane przez najwyższe szczeble w najważniejszych rosyjskich mediach państwowych. Mają bezpośrednio na celu podważenie liberalnej demokracji, państwa prawnego i praw człowieka, a także uciszenie instytucji, organizacji międzyrządowych, polityków i obywateli, którzy bronią tych wartości⁽⁹⁾.

4.3. Żyjemy w epoce silnej polaryzacji stosunków politycznych i demokratycznych. Według ośrodków analitycznych, takich jak Freedom House, Economist Intelligence Unit itd., od kryzysu gospodarczego w 2008 r. demokracja znajduje się pod rosnącą presją. Jedną z konsekwencji tego jest nowy typ przywództwa politycznego, którego profil stanowi zerwanie z demokratyczną tradycją budowaną w Europie w ciągu ostatnich 70 lat. W miejsce demokratycznie wybranego liberalnego przywództwa mamy do czynienia z coraz większą liczbą osób sprawujących władzę „silnej ręki”, których wyborowi towarzyszą wnikliwe pytania o integralność procesów, które ich wyłoniły. Zналиśmy ten rodzaj przywództwa z miejsc pozostających poza sferą wpływów UE, takich jak Rosja i Chiny. Jednakże wraz z wyborem przedstawicieli w rodzaju Trumpa, Erdogana i „nieoliberalnych demokratów” wyłonionych w państwach członkowskich UE – z których wszyscy stali się słynni z powodu swoich preferencji do dezinformacji, pogardy dla demokracji i nadszarpniętych stosunków z państwem prawnym – zjawisko to staje się bardzo głośne i niezwykle bliskie.

4.4. Odpowiednio funkcjonująca demokracja zależy od dobrze poinformowanych obywateli, dokonujących świadomych wyborów na podstawie wiarygodnych faktów i zaufanych opinii, jednak „wiarygodność” i „zaufanie” to pojęcia, które dla współczesnego społeczeństwa nie są już tak oczywiste. W tego rodzaju mocno spolaryzowanym klimacie społecznym charakteryzującym się nadmiarem informacji ludzie są bardzo podatni na dezinformację, co sprawia, że stosunkowo łatwo można manipulować ich zachowaniem. Mieliśmy już okazję obserwować tego rodzaju skutecznie przeprowadzone działania destabilizacyjne podczas wyborów powszechnych w różnych państwach członkowskich oraz w trakcie innych wydarzeń, na przykład w czasie kampanii przed referendum na temat brexitu, kampanii dezinformacyjnych dotyczących napaści na Krym i Ukrainę oraz ataku na lot nr MH 17 Malaysian Airlines za pomocą rosyjskiego systemu rakietowego BUK w 2014 r., w którym zginęli wszyscy obecni na pokładzie w liczbie 298. Zachęca się Komisję do poszukiwania bardziej proaktywnych sposobów edukowania społeczeństwa na temat zagrożeń, jakie niosą z sobą kampanie dezinformacyjne, ataki cybernetyczne, oraz na temat ogólnego wpływu działań prowadzonych z zewnątrz na społeczeństwo. Można by np. wzorować się na środkach przedsięwziętych niedawno w innych krajach i zapewnić obywatelom łatwo dostępne i atrakcyjne informacje na temat pilnych kwestii dotyczących cyberbezpieczeństwa, w tym wskazówki i przykłady sprawdzonych rozwiązań w zakresie najlepszych sposobów ochrony codziennego otoczenia cyfrowego.

⁽⁶⁾ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0272+0+DOC+PDF+V0//PL>

⁽⁷⁾ http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271

⁽⁸⁾ <http://www.consilium.europa.eu/pl/meetings/european-council/2015/03/19-20/>; <http://data.consilium.europa.eu/doc/document/ST-1-2018-INIT/pl/pdf>

⁽⁹⁾ „The Strategy and Tactics of the Pro-Kremlin Disinformation Campaign”, ESDZ.

4.5. EKES zgadza się z Komisją, że, biorąc pod uwagę złożoność kwestii i szybkie tempo rozwoju sytuacji w środowisku cyfrowym, wszelkie działania polityczne powinny być kompleksowe, stale oceniać zjawisko dezinformacji i dostosowywać cele polityczne w świetle jej ewolucji. Nie istnieje jedno rozwiązanie, które pozwoliłoby sprostać wszystkim wyzwaniom, lecz powstrzymanie się od działań nie jest wyjściem. Propozycje Komisji to krok we właściwym kierunku, ale konieczne są dalsze, bardziej skuteczne działania. Zwalczaniu dezinformacji powinny przyświecać przejrzystość, różnorodność, wiarygodność i pluralizm, przy jednoczesnej ochronie wolności słowa i innych praw podstawowych.

4.6. Rosja wydaje się być szczególnie aktywna w zakresie dezinformacji i wojny hybrydowej przeciwko Zachodowi, ze szczególnym uwzględnieniem UE. Aby temu przeciwdziałać, pilnie potrzebujemy bardziej przejrzystego, godnego zaufania i odpowiedzialnego ekosystemu internetowego. EKES zaleca korzystanie z publikacji pt. „The Prague Manual” – badania ufundowanego przez Ministerstwo Spraw Zagranicznych Królestwa Niderlandów i Międzynarodowy Fundusz Wyszehradzki, dającego jasny obraz wrogiej rosyjskiej działalności wywrotowej w UE i zagrożenia, jakie stanowi to dla demokracji. Mimo że niektóre państwa członkowskie wciąż wątpią w istnienie takiego zagrożenia lub nawet przyczyniają się do jego rozprzestrzeniania, w badaniu jasno ocenia się, że podjęcie przez Unię działań jest absolutną koniecznością. Badanie przedstawia konkretne propozycje dotyczące opracowania i wdrożenia strategii przeciwdziałania wrogim i wywrotowym wpływom.

4.7. Rola platform internetowych w zakresie dezinformacji jest moralnie naganna. W stosunkowo krótkim czasie platformy te znacząco rozwinęły swego rodzaju funkcję użyteczności publicznej podobną do tej, jaką w przeszłości pełniły przedsiębiorstwa telefoniczne, rozgłośnie radiowe i telewizyjne oraz prasa. Aby móc korzystać z „darmowych” usług serwisów platform internetowych, użytkownicy płacą swoimi danymi osobowymi, które umożliwiają platformom sprzedawanie ogromnej ilości mikroukierunkowanych reklam, jak ilustruje przypadek Cambridge Analytica. Ten wypaczony (jeśli chodzi o prywatność) model pozyskiwania przychodów jest dla platform zbyt opłacalny, żeby zrzekły się go dobrowolnie. Pojawiły się opinie sugerujące, że platformy takie jak Facebook również powinny oferować wiarygodne, dobrze działające „facebookowe” usługi, które wymagałyby od użytkowników uiszczenia przystępnej kwoty pieniężnej w zamian za gwarancję poszanowania ich prywatności. Pojawia się pytanie, czy potencjalni użytkownicy nadal wystarczająco wierzą w wiarygodność i uczciwość portali takich jak Facebook i mają do nich zaufanie po tym, jak stojące za nim przedsiębiorstwo musiało tłumaczyć się ze swojego postępowania przed Senatem USA. Aby zwiększyć publiczne zaufanie do platform internetowych i chronić obywateli przed tego rodzaju nadużyciem, w tym przed nieodpowiednim postępowaniem z danymi osobowymi oraz przed ich udostępnianiem, platformy te muszą podlegać regulacjom, jak wskazano wcześniej w przyjętym w 2016 r. kodeksie postępowania dotyczącym nielegalnego nawoływania do nienawiści w internecie, w ogólnym rozporządzeniu o ochronie danych bądź w dyrektywie w sprawie bezpieczeństwa sieci i informacji. Jednakże zaproponowana przez Komisję samoregulacja jest jedynie pierwszym krokiem w tym względzie i powinny jej towarzyszyć dalsze środki podjęte przez Komisję.

4.8. Andrew Keen, brytyjski przedsiębiorca i pisarz, który znany jest jako antychryst internetu, opublikował cztery bardzo krytyczne książki na temat rozwoju internetu. Nie jest on przeciwny internetowi lub mediom społecznościowym, ale uważa, że istotą problemu są działania dużych firm technologicznych mające na celu gromadzenie szczególnie chronionych informacji dotyczących osób. Prywatność jest bardzo cennym dobrem określającym, kim jesteśmy. Tzw. darmowy model biznesowy – w ramach którego nie płacimy pieniędzmi, ale rezygnacją z naszej prywatności – zniszczył naszą prywatność. Keen przedstawia analogię z XIX wiekiem, kiedy to rewolucja przemysłowa spowodowała zmiany w skali, którą można porównać ze skalą zmiany wywoływanej obecnie przez rewolucję cyfrową. Kiedy zmiana określana jest jako rewolucja, to zazwyczaj pociąga za sobą poważne problemy. W XIX wieku udało nam się rozwiązać te problemy przy pomocy takich narzędzi jak innowacje, regulacje, wybory konsumentów, powództwo cywilne i edukacja. W swym przesłaniu Keen wskazuje, że możemy dokonać tego ponownie przy pomocy ludzkiej – nie sztucznej – inteligencji. Musimy przy tym wykorzystać wszystkie zasoby, których użyliśmy do powstrzymania poprzedniej rewolucji, aby zapewnić kontrolę nad rewolucją cyfrową i zapobiec jej dominacji nad nami.

4.9. Na podstawie dostępnych opracowań UE powinna zapewnić i kontynuować badania w zakresie wpływu dezinformacji w Europie, również poprzez uwzględnienie w przyszłych sondażach Eurobarometru monitorowania odporności Europejczyków na dezinformację. Sondaże te powinny obejmować nie tylko ogólne dane dotyczące fałszywych informacji, lecz także pozwolić określić faktyczną odporność Europejczyków na dezinformację. Komisja nie traktuje sprawy jako naglącej i brakuje jej ambicji, dlatego nie odnosi się do zasadniczych kwestii takich jak systemy wsparcia dla tradycyjnych mediów w celu zagwarantowania podstawowego prawa obywateli do wysokiej jakości wiarygodnych informacji, zbadanie możliwości ustanowienia partnerstw publiczno-prywatnych w celu tworzenia płatnych platform internetowych oferujących bezpieczne i przystępne cenowo usługi online, przestudiowanie możliwości zapewnienia większej przejrzystości algorytmów leżących u podstaw tych systemów internetowych oraz zapewnienia większego nadzoru nad tymi algorytmami, a także zanalizowanie sposobności rozbicia monopolii w celu przywrócenia równych warunków działania dla uczciwej konkurencji, aby zapobiec stopniowemu korumpowaniu społeczeństwa.

4.10. Na przykład rozważenie możliwości stworzenia platformy internetowej opartej na partnerstwie publiczno-prywatnym gwarantującym użytkownikom prywatność mogłoby okazać się rentowne. Tego rodzaju platforma europejska z Komisją jako współfinansującym partnerem publicznym mogłaby stanowić bardzo atrakcyjną i obiecującą propozycję stanowiącą alternatywę dla maszyny manipulacyjnej Marka Zuckerberga i innych dużych monopolii prywatnych i komercyjnych z USA i Chin. Taka platforma powinna gwarantować poszanowanie prywatności swoich użytkowników.

4.11. W gospodarce rynkowej wszystko ma swoją cenę, ale zgodnie z przedstawioną alternatywą walutą byłyby tu pieniądze, a nie prywatność. Większość wymaganego budżetu na tę quasi-publiczną usługę można by finansować z wpływów podatkowych, tak jak się to dzieje w przypadku wszystkich usług publicznych. Aby sfinansować pozostałą część budżetu, użytkownicy musieliby płacić względnie niewielką kwotę pieniędzy w celu ochrony ich prywatności przed niezaspokojonym apetytem na dane osobowe obecnych platform „społecznych”. Jeśli Unia i rządy krajowe państw członkowskich oficjalnie zadeklarowałyby taką platformę jako preferowanego partnera i wykorzystały ją jako alternatywę dla obecnych drapieżników pożerających dane, to dysponowałaby ona ekonomią skali konieczną, by móc konkurować z podmiotami działającymi obecnie na rynku. UE mogłaby również wykorzystać istniejące wyszukiwarki internetowe gwarantujące pełną prywatność jako swoich preferowanych partnerów, zainstalować je jako aplikacje domyślne na wszystkich komputerach wykorzystywanych przez instytucje Unii oraz zalecić je jako aplikacje domyślne instytucjom rządowym państw członkowskich. Komisja mogłaby również odgrywać bardziej proaktywną rolę i zbadać możliwości regulacyjne odnoszące się do algorytmów oraz rozbijania monopolu.

4.12. Mimo że weryfikacja faktów nie stanowi rozwiązania problemu, to ma ona duże znaczenie. Służy jako pierwszy krok do zrozumienia, ujawnienia i analizy dezinformacji, co jest konieczne do opracowania dalszych środków zaradczych. Dużego wysiłku wymaga również pozyskanie uwagi większej grupy odbiorców, ponieważ nie każdy korzysta z platform społecznościowych czy nawet internetu. Dotarcie do mieszkańców odległych regionów może być szczególnie trudne. Ważna jest widoczność w mediach. Telewizja jest wciąż najbardziej powszechnym źródłem informacji dla ludzi, zatem regularna emisja programów objaśniających przypadki dezinformacji w językach narodowych może znacząco przyczynić się do zwiększenia świadomości społecznej tego problemu. Jest istotne, aby proces weryfikacji faktów był prowadzony przez profesjonalistów w celu uniknięcia błędów, które pojawiły się ostatnio przy pierwszej próbie podjętej przez Komisję. Problemom takim można zapobiec poprzez współpracę z wydawnictwami i organizacjami medialnymi, których dziennikarze są zaangażowani w weryfikację faktów.

4.13. Jednym z problemów związanych z dezinformacją jest brak możliwości sprawdzenia tożsamości źródeł rozpowszechniających dezinformację w internecie. Działanie w cyberprzestrzeni pod fałszywą tożsamością jest zbyt łatwe – i ogólnie właśnie tak postępują osoby, które działają w sieci w złych zamiarach. Komisja przedstawia kilka propozycji, które zostały określone we wspólnym komunikacie na temat bezpieczeństwa cybernetycznego opublikowanym we wrześniu 2017 r. Problemem jest to, że propozycje te nie są obowiązkowe – użytkownicy mogą wybrać, że chcą nawiązywać kontakty na platformach internetowych jedynie z osobami, które podały swoje dane osobowe, Komisja będzie promowała dobrowolne korzystanie z systemów bezpiecznej identyfikacji dostawców informacji itd. Oczywiście potencjalnie może dojść do konfliktu interesów pomiędzy zachowaniem prywatności a pełną kontrolą, więc należy umożliwić zachowanie anonimowości podczas biernego przeglądania internetu. Jeśli jednak rzeczywiście chcemy poczynić postępy w walce z dezinformacją, być może będziemy potrzebowali ostrzejszych środków dotyczących identyfikacji w przypadku osób aktywnie działających w internecie. Ostatecznie, zgodnie z kodeksem z Bordeaux z 1954 r., uchwalonym przez Międzynarodową Federację Dziennikarzy, który określa jasne i ścisłe zasady pracy ze źródłami, to właśnie jest sposób funkcjonowania wysokiej jakości mediów informacyjnych. Czasami istnieją uzasadnione przyczyny, dla których tradycyjne organizacje zapewniające wysokiej jakości media informacyjne publikują informacje z anonimowego źródła, jednak zawsze zamieszczają adnotację, że nazwisko i adres źródła są znane redakcji.

4.14. Technologie nie są ani „złe”, ani „dobre” – są neutralne. Mogą być używane w dobry lub zły sposób, ale to jest zależne od wyborów ludzi z nich korzystających. Nowo powstające technologie, takie jak te wykorzystywane obecnie w sztuce dezinformacji, mają również potencjał do odgrywania kluczowej roli w jej zwalczaniu. Dlatego też EKES z zadowoleniem przyjmuje wyrażony przez Komisję zamiar pełnego wykorzystania planu prac programu „Horyzont 2020” oraz jego następcy, programu „Horyzont Europa”, do uruchomienia w przyszłości badań i technologii takich jak sztuczna inteligencja, technologia łańcucha bloków i algorytmy w celu lepszej identyfikacji źródeł, weryfikowania wiarygodności informacji oraz oceny trafności i jakości źródeł danych. Jednakże kluczowe znaczenie przypada szczegółowym analizom innych możliwości finansowania na rzecz przeciwdziałania dezinformacji, ponieważ większość inicjatyw nie ma zastosowania do programów „Horyzont”.

4.15. Bezpieczne i odporne procesy wyborcze są podstawą demokracji w UE, ale ich bezpieczeństwa i odporności nie można już zagwarantować. W ostatnich latach podczas wyborów w co najmniej 18 krajach wykryto działania manipulacyjne i dezinformacyjne w internecie, a taktyka dezinformacji przyczyniła się do ogólnego spadku wolności internetu przez siódmy rok z rzędu. EKES z zadowoleniem przyjmuje inicjatywy Komisji podjęte w celu określenia najlepszych praktyk w zakresie rozpoznawania zagrożeń dla procesu wyborczego związanych z cyberatakami i dezinformacją oraz ich łagodzenia i zarządzania nimi z myślą o wyborach do Parlamentu Europejskiego w 2019 r.

4.16. Umiejętności cyfrowe i umiejętności w zakresie korzystania z mediów, jak również edukacja obywatelska to kluczowe elementy służące zwiększeniu odporności społecznej, uwzględniając w szczególności, że licznie obecni na platformach internetowych młodzi ludzie są podatni na dezinformację. Za politykę edukacyjną odpowiedzialny jest rząd, dlatego zadanie organizowania tego na wszystkich szczeblach krajowego systemu edukacji oraz przeszkolenie nauczycieli w tym zakresie spoczywa na rządach krajowych. Niestety rządy w swoich programach politycznych rzadko w ramach krajowego systemu edukacji nadają istotną pozycję edukacji w zakresie umiejętności korzystania z mediów i z informacji.

Należy to poprawić w pierwszej kolejności, jednak umiejętność korzystania z mediów i z informacji wykracza poza system edukacji. Należy ją promować i poprawiać we wszystkich grupach społecznych, bez względu na wiek. Pewną rolę w tych obszarach powinny odgrywać organizacje pozarządowe. W całej Europie działa już wiele takich organizacji, ale większość z nich funkcjonuje na małą skalę i nie ma koniecznego zasięgu. Lukę tę mogłyby wypełnić krajowe inicjatywy współpracy pomiędzy organizacjami pozarządowymi a rządami krajowymi.

4.17. Wysokiej jakości media informacyjne oraz wiarygodne dziennikarstwo odgrywają ważną rolę w zapewnianiu obywatelom rzetelnych i zróżnicowanych informacji. Te tradycyjne media borykają się z problemami finansowymi, ponieważ platformy rozpowszechniają treści stworzone przez tradycyjne media bez zwracania poniesionych przez nie kosztów, a następnie przejmują ich zyski przez sprzedaż reklam. Wskazane byłoby dojście do szybkiego porozumienia w sprawie unijnej reformy prawa autorskiego, aby poprawić sytuację wydawców i zagwarantować, że posiadacze praw będą wynagradzani za swoją pracę, jeżeli jej owoce są wykorzystywane przez innych w celach komercyjnych. Ponadto zaleca się poszukiwanie rozwiązań w celu rozszerzenia zakresu zapowiedzianej przez Parlament Europejski we wrześniu 2018 r. inicjatywy w sprawie europejskiego finansowania przeznaczonego konkretnie na wsparcie dziennikarstwa śledczego w UE. Silna i wiarygodna prasa jest podstawą odpornej i dającej się obronić demokracji, w której nadal docenia się wartości prawdy i rozliczalności. Finansowanie jest szczególnie ważne dla mniejszych środków przekazu, które często stają w obliczu powództw i dokuczliwych roszczeń mających na celu ich zamknięcie.

4.18. Aby zwalczać wewnętrzne i zewnętrzne zagrożenia wynikające z dezinformacji, Komisja powołała w 2015 r. grupę zadaniową East StratCom, mającą skupiać się na aktywnej komunikacji strategicznej dotyczącej polityk Unii w celu przeciwdziałania próbom destabilizacji podejmowanym przez Rosję. EKES z zadowoleniem przyjąłby większą aktywność Komisji w informowaniu ogółu społeczeństwa o działaniach East StratCom i nakierowywaniu na informacje zawarte na stronie internetowej tej grupy zadaniowej, aby zwiększyć świadomość społeczną na temat zagrożeń dla naszej demokracji i wzmocnić odporność na te zagrożenia. Konieczne jest również zwiększenie budżetu tej grupy zadaniowej. W październiku 2017 r. Parlament Europejski przyjął budżet w wysokości 1 000 000 EUR. Jego wysokość jest ledwo porównywalna ze środkami finansowymi zainwestowanymi przez innych uczestników, takich jak Federacja Rosyjska. (Departament Stanu USA szacuje, że wyrafinowane wysiłki Kremla, by wpływać na kampanie wyborcze, obejmują wewnętrzny i zewnętrzny aparat propagandowy pochłaniający 1,4 mld USD rocznie, który rzekomo dociera do około 600 mln ludzi w 130 krajach i w 30 językach).

4.19. Poza innymi działaniami zachęca Komisję do zwrócenia uwagi na to, że instytucje krajowe i przepisy w zakresie bezpieczeństwa informacji w państwach członkowskich są często niedostatecznie rozwinięte, a otoczenie prawne jest przestarzałe, co uniemożliwia właściwym agencjom regulacyjnym odpowiednie kontrolowanie kanałów działalności dezinformacyjnej pod kątem ich zgodności z normami ustawodawczymi. Ponadto współpraca międzyinstytucjonalna jest niewystarczająca, a także istnieje wyraźny brak krajowych strategii długoterminowych mających na celu zwalczanie prowadzonych z zewnątrz kampanii dezinformacyjnych i przygotowanie spójnych przekazów dla najbardziej narażonych grup ludności. Ważną kwestią jest także szczegółowy przegląd unijnej dyrektywy o audiowizualnych usługach medialnych, zgodnie z którą środki przekazu mogą być zarejestrowane w jakimkolwiek państwie członkowskim, jeśli jeden z członków zarządu spółki medialnej zamieszkuje w tym kraju, dyrektywa ta bowiem umożliwia dotarcie do odbiorców w państwach europejskich z jednoczesnym wykorzystaniem luk w przepisach UE.

Bruksela, dnia 19 września 2018 r.

Luca JAHIER
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego

ZAŁĄCZNIK

Następująca poprawka, która uzyskała poparcie co najmniej jednej czwartej oddanych głosów, została odrzucona w trakcie debaty:

Punkt 4.3

4.3. ~~Żyjemy w epoce silnej polaryzacji stosunków politycznych i demokratycznych. Według ośrodków analitycznych, takich jak Freedom House, Economist Intelligence Unit itd., od kryzysu gospodarczego w 2008 r. demokracja znajduje się pod rosnącą presją. Jedną z konsekwencji tego jest nowy typ przywództwa politycznego, którego profil stanowi zerwanie z demokratyczną tradycją budowaną w Europie w ciągu ostatnich 70 lat. W miejsce demokratycznie wybranego liberalnego przywództwa mamy do czynienia z coraz większą liczbą osób sprawujących władzę „silnej ręki”, których wyborowi towarzyszą wnikliwe pytania o integralność procesów, które ich wyłoniły. Znaliliśmy ten rodzaj przywództwa z miejsc pozostających poza sferą wpływów UE, takich jak Rosja i Chiny. Jednakże wraz z wyborem przedstawicieli w rodzaju Trumpa, Erdogana i „neliberalnych demokratów” wyłonionych w państwach członkowskich UE — z których wszyscy stali się słynni z powodu swoich preferencji do dezinformacji, pogardy dla demokracji i nadszarpniętych stosunków z państwem prawnym — zjawisko to staje się bardzo głośnie i niezwykle bliskie.~~

Wynik głosowania

Za: 68

Przeciw: 82

Wstrzymało się: 24
