

PROTOKÓŁ z XIII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 16 lipca 2021 roku, o godzinie 13:00 w formie wideokonferencji.

Sztuczna inteligencja (AI): omówienie dokumentów KE – Pan Mateusz Tykierko.

21 kwietnia Komisja Europejska ogłosiła dwa komunikaty - Komunikat COM(2021)205 Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów o rozwoju sztucznej inteligencji i europejskiego podejścia do sztucznej inteligencji oraz rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii COM (2021) 206. Zawartość komunikatu wskazuje wagę AI dla rozwoju UE, szanse i ryzyka, przedstawia europejskie podejście do AI, kładzie nacisk na wartości europejskie w szczególności prawa człowieka oraz wiarygodne rozwiązania AI. Komunikat pierwszy wprowadza akt w sprawie sztucznej inteligencji oraz modyfikuje plan na rzecz AI opublikowany w 2018 r. Definiuje wygląd systemów o wysokim stopniu ryzyka oraz inne systemy, które powinny zawierać odpowiednią transparentność z punktu widzenia użytkowników. Proponuje też „piaskownice regulacyjne”. KE planuje nakłady inwestycyjne w wysokości 1 mld EUR rocznie oraz osiągnięcie 20 mld rocznie poprzez aktywizację sektora prywatnego i państw członkowskich. Wskazywane są: Program Odbudowy, Cyfrowa Europa, Horyzont Europa czy Program Spójności.

Kraje członkowskie i KE wskazują, że program należy przyspieszać, działać strategicznie i podchodzić tak do polityk, aby zajmować się wyzwaniami globalnymi. Wskazywane są cztery obszary, a dla każdego z nich, opisywany jest stan podjętych działań. Ujęte są także plany Komisji oraz rekomendacje dla krajów członkowskich, jeżeli chodzi o działania, które należy podjąć w tych obszarach. Na końcu znajdują się dwa załączniki: tabelaryczne zestawienie planu dla kluczowych działań oraz zestawienie i omówienie wprowadzonych krajowych strategii AI.

Pierwszy obszar - sprawianie, aby warunki dla rozwoju AI były odpowiednie poprzez inwestowanie w firmy, ale głównie w infrastrukturę i całą przestrzeń związaną z danymi i w zasoby obliczeniowe. Drugi obszar mówiący o tym, aby powstawały centra kompetencji w ramach poszczególnych krajów. Trzeci obszar to skupienie się na ludziach i działania dla dobra społeczeństwa, głównie z punktu widzenia informowania, rozbudowy kompetencji potrzebnych do budowy, tworzenia i wdrażania wiarygodnych systemów sztucznej inteligencji. Czwarty obszar mówiący o strategicznych zakresach, które są istotne z punktu widzenia UE.

Należy zadbać, aby w Polsce była jak najlepiej zagospodarowana odpowiednia krytyczna infrastruktura obliczeniowa na potrzeby rozbudowy i utrzymania AI. Przykłady w jaki sposób KE będzie wspierała i jakie działania podejmie dla poszczególnych obszarów pokaże wprowadzenie *Data Act* oraz *European data spaces and the European cloud federation*. Wskazywany jest mechanizm *Important Projects of Common European Interest*, który w

Polsce jest obecny w postaci IPCEI chmurowego. Jeżeli chodzi o obecną dostępność infrastruktury obliczeniowej na potrzeby naukowe i komercyjne, jesteśmy w dobrym miejscu, z uwagi na inwestycje, które są prowadzone do 2023 r.

Co do europejskiej pozycji w procesorach i technologiach półprzewodnikowych – być może należałoby stworzyć raport i zdecydować, czy Polska ma potencjał w tych technologiach. KE będzie wspierała *Testing and Experimentation Facility* w ramach *Digital Europe Programme*. Warto przyrzeć się kompetencjom cyfrowym oraz ochronie zdrowia i sposobie ich realizowania.

Następnie omówiono akt w sprawie sztucznej inteligencji COM (2021) 206 wprowadzony przez poprzedni komunikat. Celem jest zharmonizowanie przepisów dotyczących AI oraz zapewnienie bezpiecznej, wiarygodnej i etycznej AI z zachowaniem wartości europejskich i transparentności. Akt zawiera ustalenie procesów i ról do zapewnienia kontroli jakości przy wdrażaniu i użytkowaniu rozwiązań AI: wprowadzenie jednolitych ram prawnych w UE, deklaracje zgodności, oznakowanie CE, piaskownice regulacyjne w zakresie AI, krajowe organy nadzorcze, unijną bazę danych systemów i procesów AI wysokiego ryzyka. Definiuje obowiązki poszczególnych podmiotów. Główny nacisk tego dokumentu - ukierunkowanie na potrzeby i prawa człowieka.

Podjęcie ma być oparte na analizie ryzyka i przypadkach użycia, a nie na technologiach. Prowadzona jest klasyfikacja systemów AI, systemom wysokiego ryzyka poświęcono największą część tego dokumentu. Dotyczy on dostawców rozwiązań AI z UE, spoza niej - jeżeli system dotyczy użytkowników z UE, importerów i dystrybutorów rozwiązań w UE; dostawców i użytkowników, którzy mają siedzibę w państwie trzecim, w zakresie, w jakim wyniki działania tych systemów są wykorzystywane w UE. Nie dotyczy zastosowań wojskowych oraz organów publicznych państwa trzeciego i organizacji międzynarodowych działających w ramach zawartych na szczeblu krajowym lub europejskim umów międzynarodowych o współpracy organów ścigania i wymiarów sprawiedliwości. Proces ratyfikacji i implementacji zakładany jest na 2-3 lata.

O zakazanych praktykach w zakresie AI mówi art. 5 – definiuje np. techniki podprogowe będące poza świadomością użytkownika w celu istotnego zniekształcenia jego zachowania w sposób, który powoduje lub może powodować u niej lub u innej osoby szkodę psychiczną lub fizyczną, ocenę lub klasyfikację ich wiarygodności. Są również wskazania dla systemów identyfikacji biometrycznej - do czego nie mogą być używane lub do czego mogą.

Następnie omówiono art. 6: systemy wysokiego ryzyka, które wynikają albo z załącznika II mówiącego o zharmonizowanych przepisach, albo z załącznika III zawierającego listę typów systemów uznawanych jako systemy wysokiego ryzyka.

Są odpowiednie paragrafy opisywania systemów dla ścigania przestępstw, dla migracji, azylu, wymiaru sprawiedliwości i procesów dydaktycznych. W rozdziale 2 zapisane są wymogi dotyczące systemów wysokiego ryzyka – co powinien spełniać oraz jak powinien zostać wdrażany. Systemy AI wymagają ponadto przejrzystości i wskazują wprost, że

dostawcy dla takich systemów powinni informować, że prowadzą np. interakcje z systemem AI. To samo dotyczy np. kategoryzacji biometrycznej dla osób fizycznych.

Obecny na posiedzeniu Pan mec. Robert Kroplewski wskazał, że na ten moment KPRM zgłosiło w uzgodnieniach do Komitetu ds. Europejskich stanowisko rządu. Dokument jest w wersji roboczej. Komunikat UE to zwieńczenie 3-letniej pracy. Szczególną uwagę zwrócono na Komunikat ekonomiczny - jest to interwencja strategiczna w obszarze ekonomii i wsparcia budowy zaufanej AI w UE. Nowe kwestie, to obszar rolnictwa oraz *tef* (Test and Experimentation Facilities) - centra testowania i walidacji technologii i piaskownice regulacyjne w obszarze transportu. Co ważne, dla celów finansowania został podjęty program *Recovery and Resilience Plan*, co pozwala KPO i środki z Funduszu Spójności potraktować jako wsparcie rozwoju AI.

Jeśli chodzi o regulacje, to z punktu widzenia Polski, jest problematyczne, aby przyjąć tak szeroką definicję AI. Zmierzamy w kierunku zawężenia tej definicji, aby nie każdy algorytm był uznawany za AI, ponieważ doszłoby do erozji pojęcia sztucznej inteligencji oraz zamrożenia rynku. Innym problemem jest, na ile te regulacje spowodują wyhamowanie inwestycji w Polsce oraz w Europie. Skoordynowany plan finansowy ma niwelować tego typu ryzyko. Takie podejście jest ważne i zaczyna być doceniane przez partnerów z OECD i USA.

Polska jest też za tym, by każdy podmiot spoza Europy, który operuje systemem AI na terenie Europy musiał zachować te same zasady, tzn. wejście na rynek tylko wtedy, gdy stworzy taki sam system AI. Co do systemu biometrycznego uważamy, że jest zbyt duża orientacja jego definicji na dane osobowe, a nie na wpływ na osobę.

Polska będzie musiała ustanowić swój organ nadzoru. Europejskim organem nadzoru jest Europejski Inspektor Danych Osobowych. W rozporządzeniu przewiduje się tzw. akty delegowane, na temat aktualizacji technologii, które stanowią wysokie ryzyko oraz listy technologii AI. Dokument taki będzie wydawany raz na dwa lata przez KE. MSZ oraz resorty związane z polityką ekonomiczną UE negatywnie się do tego odniosły. Grupy robocze przy KPRM również brały udział w konsultacjach i wydały swoje opinie z obszaru bezpieczeństwa, innowacyjności i badań, zdrowia, legislacji oraz prawa. Z chwilą przyjęcia stanowiska Polski staną się one materiałem obowiązującym dla naszej delegacji.

Konsorcja międzynarodowe (złożone minimum z trzech krajów członkowskich) mogą się składać z dowolnych podmiotów, nie tylko instytucji naukowych i firm. Nasze państwo musi zadeklarować 50 % wkładu (drugie 50% z KE). Aby ktoś mógł być członkiem konsorcjum TEF, musi wykazać poprzez praktykę i doświadczenie, że ma możliwość prowadzenia testów bądź posiada wiedzę w obszarze certyfikowania lub walidacji wyzwań testowych w obszarze AI i innych (transport, medycyna, rolnictwo itd.).

Dokument „*Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*” został przyjęty jako dokument koordynujący programy działań, a za jego wdrożenie odpowiada Centrum GovTech.

Omówienie projektów aktów prawnych KE - Digital Services Act oraz Digital Markets Act - Pani Katarzyna Chałubińska-Jentkiewicz oraz Pan Michał Kanownik.

Pani K. Chałubińska-Jentkiewicz omówiła rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (DSA), który zmienia Dyrektywę o handlu elektronicznym 2000/31 Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. *w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego*. DSA ma na celu przede wszystkim ujednolicenie funkcjonowania rynku usług cyfrowych i zapewnienie skutecznego nadzoru nad usługodawcami działającymi w internecie. Cele przedstawione w rozporządzeniu to m.in. poprawa funkcjonowania rynku, zwiększenie bezpieczeństwa i ochrona wolności wypowiedzi w internecie, zwiększenie przejrzystości działania platform internetowych, np. w obszarze reklamy internetowej i moderowania treści, zagwarantowanie, żeby bardzo duże platformy internetowe działały w sposób odpowiedzialny w celu ograniczenia ryzyka wynikającego z korzystania z ich usług. Wprowadzono definicję platformy internetowej.

Gradacja odpowiedzialności i obowiązków jest widoczna w całym dokumencie i odzwierciedla się przede wszystkim w kompetencjach i obowiązkach. Zwrócono uwagę na powtarzające się w regulacjach unijnych kwestie dotyczące udostępniania najważniejszych danych. DSA rozwiązuje problem odpowiedzialności za przechowywane dane i informacje. Wprowadza też obowiązki identyfikowania sprzedawców nielegalnych towarów, a także nowe obowiązki identyfikacji użytkowników biznesowych na internetowych platformach handlowych oraz środki, które służą zwalczaniu nielegalnych towarów, usług i treści w internecie.

Zwrócono uwagę, że rozporządzenie nie wprowadziło definicji treści nielegalnych. Polski rząd zaproponował wprowadzenie klauzuli - wszystko, co jest niedozwolone offline powinno być również niedozwolone online. Wpisanie takiej zasady wzmocni cel oraz przesłanie całej regulacji, ale również pozwoli uniknąć w przyszłości wątpliwości interpretacyjnych. Samo rozporządzenie określa usługi pośrednictwa, jako ogólnie przyjętą regułę, która obejmuje wszystkich dostawców dostępu do internetu, rejestrów nazw domen, usług hostingowych (takich jak usługi w chmurze i webhosting), platformy internetowych (w tym bardzo dużych).

Nowych unijnych przepisów będą musieli przestrzegać wszyscy pośrednicy internetowi oferujący swoje usługi na jednolitym rynku, bez względu na to czy mają siedzibę w UE, czy poza jej terytorium. Każdy dostawca usługi pośredniej z siedzibą w UE będzie podlegał nadzorowi jednego lub więcej koordynatorów ds. usług cyfrowych. W projekcie DSA wprowadzono rozwiązania dotyczące transgranicznej współpracy krajowych koordynatorów. Bardzo duże platformy będą miały nowe i ważne obowiązki, m.in. współpracę w zakresie reagowania kryzysowego.

Użytkownicy m.in. będą informowani o usunięciu treści przez platformy i będą mogli to zakwestionować, a także mieć większe bezpieczeństwo i więcej informacji o faktycznych sprzedawcach. Wprowadzono również surowsze obowiązki dla bardzo dużych platform na poziomie ogólnej organizacji serwisu, jeżeli chodzi o ocenę i ograniczanie ryzyka dla praw

użytkowników. Przedsiębiorcy są zachęceni do tego, żeby chronić swoich użytkowników przed nielegalnymi treściami, towarami i usługami. Będą korzystać z nowych prostych i skutecznych mechanizmów służących do sygnalizowania nielegalnych treści i towarów naruszających prawo, w tym prawo własności intelektualnej, lub które stanowią nieuczciwą konkurencję. Rząd RP zaproponował większe kompetencje dla regulatorów krajowych tak, aby zapewnić odpowiedni nadzór nad działalnością platform internetowych.

Stanowisko Rządu RP mówi także, że zarządzanie treścią przez duże platformy powinno uwzględniać w jak największym stopniu kontekst społeczno-kulturowy kraju użytkownika. Ten musi mieć prawo do szybkiej ścieżki sądowej. Regulaminy świadczenia usługi powinny być publikowane w zrozumiałym, czytelny i przyjazny użytkownikowi sposób.

Rząd RP zwrócił uwagę na przesłankę uwzględnienia „kontekstu społeczno-kulturowego”. Przyjęto jednak, że ten postulat stoi w sprzeczności z założeniami rozporządzenia DSA, a projekt DSA przewiduje należyte zabezpieczenie praw użytkowników poprzez uregulowanie ścieżki odwoławczej dotyczącej blokowania treści przez dostawcę usługi hostingu, w tym platformy internetowej. Duże platformy internetowe powinny podjąć większy wysiłek na rzecz zwalczania szkodliwych treści, w tym dezinformacji.

W zasadę harmonizacji rynku wewnętrznego godzi zgłoszony również przez rząd RP postulat kompetencji regulatora krajowego do żądania od bardzo dużej platformy uzgadniania z regulatorem warunków korzystania z oferowanych przez platformę usług.

Wspomniano, że w rozporządzeniu powinno znaleźć się zabezpieczenie wydawania ogólnoeuropejskich nakazów usuwania treści, jeżeli naruszają one prawo krajowe jedynie części państw członkowskich. Rząd RP pozytywnie odbiera obowiązki wskazywane w art. 21 DSA, np. połączenie obowiązków informowania i natychmiastowego przekazywania wszystkich dostępnych platformie informacji na temat możliwego przestępstwa, co wpłynie pozytywnie na wykrywalność i zwalczanie przestępczości. W toku prac nad DSA ustalono w stanowisku Rządu, że należy spójnie stosować różne regulacje względem tych samych podmiotów. Podkreślono, że występują nadal problemy interpretacji DSA, także w zakresie tego, kto ma być odpowiedzialny i za co.

Pan Przewodniczący wniósł uwagę na analizy wskazujące na to, że Donald Trump nie ma realnych szans na zwycięstwo w sądzie w sprawie zablokowania jego konta przez bardzo duże platformy, ponieważ wolność słowa jest chroniona w Stanach Zjednoczonych tylko wtedy, gdy to państwo zabiera wolność słowa. Bardzo duże platformy nadają sobie kompetencje organów państwa. Jeśli duża platforma blokuje konto politykowi, to nie może on prowadzić kampanii wyborczej w żadnej miejscowości, ponieważ wójt/ burmistrz może zakazać tego, powołując się na decyzje platform. Należy zaproponować takie zmiany prawne, które odejmą bardzo dużym platformom bezkarną możliwość decyzji wkraczających w dotychczasowe kompetencje państwa dotyczące wolności obywatelskiej.

Pan M. Kanownik wyjaśnił, że *Digital Markets Act* (DMA) jest to uzupełnienie dokumentu o usługach cyfrowych DSA. Na razie brak jasności w nowych przepisach i ich stabilności. DMA

wprowadza dodatkowe regulacje w kilku elementach. Reguluje rynek dużych platform, wprowadza szereg korzystnych regulacji z punktu widzenia małego i średniego przedsiębiorcy, który korzysta z ich usług. Za nieprzestrzeganie regulacji DMA wprowadzane są bardzo duże kary. Natomiast niektóre regulacje mogą grozić zahamowaniem procesu cyfryzacji europejskiej gospodarki i wprowadzania nowoczesnych technologii. Jedną ze słabości DMA jest regulacja *ex ante* dotycząca instytucji Strażników Dostępu - kluczowego pojęcia definiującego największe platformy na rynku, na które będą powierzone obowiązki regulacyjne.

Toczy się dyskusja w Komisji Europejskiej na bazie jakich przepisów DMA ma zostać wdrożone oraz jaką ma mieć podstawę traktatową. KE dyskutowała, czy oprzeć DMA o podstawę traktatową dotyczącą konkurencji, czy funkcjonowania rynku wewnętrznego. KE zaproponowała, żeby zastosować w tym zakresie artykuł 114 traktatu, który umożliwi KE uniknięcie wymogu jednomyślności wśród państw członkowskich.

Polskie stanowisko w sprawie DMA mocno ewoluowało, z początku skupiało się na kwestii największych platform, później zostało uzupełnione o małe i średnie firmy. Obawy Rządu to: wprowadzenie mechanizmu aktów delegowanych do rozporządzenia w sprawie wyznaczania strażników dostępu, zmiany katalogów praktyk zakazanych, potencjalny wzrost kosztów dla małych i średnich firm; ogromna niejasność zapisów i zbyt duże znaczenie mechanizmu *ex ante*, swoboda regulowania rynku oddana w ręce Komisji Europejskiej.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Andrzej Dulka
4. Agnieszka Gryszczyńska
5. Michał Kanownik
6. Janusz Kosiński
7. Karol Krawczyk
8. Anna Beata Kwiatkowska
9. Dariusz Milka
10. Aleksandra Musielak
11. Józef Orzeł - Przewodniczący
12. Bolesław Piasecki
13. Paweł Śniatała
14. Mateusz Tykierko
15. Marcin Zarzecki

Zaproszeni goście:

16. Wiesław Paluszyński, ekspert Rady

Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

17. Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa w KPRM
18. Anna Biała, Zastępca Dyrektora Departamentu Rozwiązań Innowacyjnych w KPRM
19. Michał Przymusiński, Zastępca Dyrektora Departamentu Rozwoju Usług w KPRM,
20. Robert Kroplewski, Pełnomocnik Ministra Cyfryzacji ds. społeczeństwa informacyjnego
21. Ewa Świętochowska, Koordynator zespołu, Departament Rozwiązań Innowacyjnych w KPRM
22. Sylwia Stefaniak, Ekspertka, Departament Rozwiązań Innowacyjnych w KPRM
23. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczypospolitej Polskiej
24. Jacek Paziewski, Dyrektor Departamentu Architektury Informacyjnej Państwa w KPRM

25. Monika Skrzyńska, Zastępca Dyrektora Departamentu Architektury Informacyjnej Państwa w KPRM
26. Anna Supeł, KPRM
27. Joanna Laskowska, KPRM