Konferencja parlamentarna
Bezpieczeństwo cybernetyczne, ochrona danych, sztuczna inteligencja: jakie wyzwania dla Europy?

zorganizowana przez francuski Senat, niemiecki Bundesrat i polski Senat

Czwartek, 20 czerwca 2019 r.

Spis treści

Przemówienia inauguracyjne

Pan Jean BIZET
Senator departamentu Manche, przewodniczący senackiej Komisji Spraw Europejskich

Pani Przewodnicząca,

Panowie Przewodniczący,

Panie Sekretarzu Generalny,

Panie Dyrektorze Generalny,

Moi Szanowni Koledzy,

Szanowni Państwo,

Z wielką przyjemnością witam Państwa dzisiaj rano w Pałacu Luksemburskim na naszej konferencji parlamentarnej, która gromadzi drugie izby parlamentarne Niemiec, Polski i Francji.

W ramach parlamentarnego wymiaru „Trójkąta Weimarskiego" francuski Senat, niemiecki Bundesrat i polski Senat postanowiły zorganizować serię trzech konferencji parlamentarnych poświęconych zagadnieniom cyfrowym. Pierwsza konferencja na temat zwalczania mowy nienawiści w Internecie i bezpieczeństwa cybernetycznego odbyła się w Warszawie w dniu 4 grudnia 2017 r. W dniu 22 października 2018 r. w Berlinie zorganizowano drugą konferencję na temat walki z fałszywymi wiadomościami.

Francuski Senat z wielką przyjemnością gości dziś trzecią konferencję zatytułowaną „Bezpieczeństwo cybernetyczne, ochrona danych i sztuczna inteligencja: jakie wyzwania dla Europy?"

Cieszę się, że ramy naszej dyskusji zostały opracowane w ten sposób: po pierwsze, dlatego, że zachęcają nas one do stawiania czoła wyzwaniom technologicznym związanym z rozwojem Internetu, rozprzestrzenianiem danych i postępem w dziedzinie sztucznej inteligencji, a także politycznym wyzwaniom w zakresie bezpieczeństwa i ochrony, które towarzyszą wchodzeniu w tę nową erę technologiczną. Po drugie, dlatego, że temat ten od razu umieszcza tę kwestię na odpowiednim poziomie, a mianowicie na szczeblu europejskim. Rewolucja przemysłowa reprezentowana tutaj przez sztuczną inteligencję głęboko przekształca nasze gospodarki i społeczeństwa oraz dotyka kwestii etycznych stanowiących wyzwanie dla europejskiego systemu wartości jako całości. Unia Europejska dysponuje obecnie dziesiątkami miliardów podłączonych urządzeń cyfrowych produkujących ogromne ilości danych narażonych na wirusy i awarie techniczne.

Braki w zakresie bezpieczeństwa i brak przejrzystości algorytmów powodują znaczne szkody dla przedsiębiorstw, zarówno pod względem ekonomicznym, jak i oczywiście pod względem reputacji, ale również pod względem szkód z powodu, których cierpią ludzie, a także budzą drażliwe pytania dotyczące kwestii odpowiedzialności. Możemy tutaj zacytować błąd informatyczny, który spowodował konieczność zniszczenia rakiety Ariane 5 w 1996 r., autopilota „zabójcę" Tesli, wykorzystanie przestarzałego systemu operacyjnego, który pozwolił złośliwemu oprogramowaniu Petya spowodować ogromne szkody w Narodowej Służbie Zdrowia a także włamania poprzez ultradźwięki do cyfrowych asystentów kontrolujących wszystko w inteligentnych domach.

W tym kontekście potrzebna jest wieloaspektowa reakcja Europy. Powiedziałbym nawet, że ta odpowiedź ma charakter strategiczny, w kontekście, w którym inni główni gracze w znacznym stopniu polegają na nowych technologiach.

Wydaje się, że Unia Europejska zdała sobie sprawę ze związanych z tym wyzwań, zarówno w kwestii bezpieczeństwa cybernetycznego, które jest przedmiotem naszego

pierwszego okrągłego stołu, jak i sztucznej inteligencji, którą zajmie się nasz drugi okrągły stół. W związku z tym we wrześniu 2017 r. Komisja Europejska zaproponowała pakiet środków mających na celu wzmocnienie odporności Unii Europejskiej w dziedzinie bezpieczeństwa cybernetycznego. Europejska ustawa o bezpieczeństwie cybernetycznym, ostatecznie przyjęta zaledwie dwa miesiące temu, zapewnia europejskie ramy certyfikacji bezpieczeństwa cybernetycznego i wzmacnia rolę Europejskiej Agencji Bezpieczeństwa Sieci i Informacji, ENISA, utworzonej w 2004 r.

Rozporządzenie to, które jest bezpośrednio stosowane w państwach członkowskich, stanowi decydujący krok naprzód w kierunku europejskiej autonomii strategicznej. Francuski Senat poparł ją europejską rezolucją z maja 2018 r., podkreślając jednocześnie znaczenie, jakie zachowują również krajowe agencje bezpieczeństwa cybernetycznego w kwestiach suwerenności.

Następnie w kwietniu 2018 r. Komisja Europejska zaproponowała, skoordynowane wspólnie z państwami członkowskimi podejście, w celu jak najlepszego wykorzystania możliwości oferowanych przez sztuczną inteligencję. Strategia ta opiera się na trzech filarach: wzmacnianie zdolności przemysłowych i technologicznych Unii Europejskiej, przygotowanie do zmian gospodarczych i społecznych spowodowanych sztuczną inteligencją oraz zapewnienie odpowiednich ram etycznych i prawnych w celu stworzenia środowiska zaufania i odpowiedzialności wokół tej technologii. Rada zatwierdziła to podejście w czerwcu 2018 r.

Jednocześnie 28 maja 2018 r. weszła w życie ogólna dyrektywa w sprawie ochrony danych osobowych (RODO), której powstanie zajęło siedem lat. To europejskie rozporządzenie, negocjowane przez cztery lata, zostało opracowane w oparciu o trzy cele: wzmocnienie praw osób fizycznych, zapewnienie rozliczalności podmiotów przetwarzających dane oraz uwiarygodnienie przepisów dzięki ściślejszej współpracy między organami ochrony danych. Te ramy prawne, które zastąpiły 28 przepisów krajowych, stanowią obecnie najwyższe światowe standardy ochrony danych osobowych w erze cyfrowej. Często podkreślam, że Unia Europejska jest o krok do przodu pod względem etycznym i możemy być zadowoleni z tego sukcesu.

Komisja Spraw Europejskich Senatu Republiki Francuskiej była zaangażowana w ten rozwój: już 19 października 2017 r. powołała grupę roboczą, której zadaniem było zbadanie kwestii wyzwań jakie stanowi sztuczna inteligencja dla Unii Europejskiej. Grupa ta sporządziła sprawozdanie pod wymownym tytułem „Sztuczna inteligencja: pilna potrzeba europejskich ambicji”. Nasz kolega, André Gattolin, przedstawi Państwu jego konkluzje w sposób bardziej szczegółowy podczas drugiego okrągłego stołu dzisiaj rano.

Chciałbym niemniej podkreślić główny wniosek wypływający z tego sprawozdania: teraz, gdy Unia Europejska przygotowała się z punktu widzenia prawa do bitwy o poprawę bezpieczeństwa cybernetycznego i ochronę danych. Europa musi zdecydowanie zaangażować się wraz z państwami członkowskimi we wdrażanie sztucznej inteligencji na skalę przemysłową.

Unia Europejska nie może przegapić tej okazji. Ma ogromny potencjał w zakresie talentów oraz badań i rozwoju. A jednak niszczy go na naszych oczach: jak wytłumaczyć, że pozwala amerykańskim gigantom cyfrowym przejmować młode, innowacyjne firmy? Dlaczego ważne kontrakty na cyfrowe zamówienia publiczne, w tym w dziedzinie edukacji, są udzielane podmiotom amerykańskim i pozaeuropejskim, umacniając w ten sposób ich pozycję dominującą? Przecież w celu wspierania wprowadzania europejskich innowacji w dziedzinie sztucznej inteligencji kluczowe znaczenie ma zapewnienie dostępu do rynku o wystarczającej wielkości: im więcej zebranych danych, tym bardziej nauka algorytmów poprawi się. Interoperacyjność zapewniana przez transfer danych między operatorami jest również istotnym elementem sukcesu nowych ekosystemów, na przykład cyfrowej przestrzeni zdrowia.

Zdecydowane zaangażowanie Europy w konkurencję w dziedzinie sztucznej inteligencji oznacza zatem wielokierunkową mobilizację wszystkich stron. Aby dać Europie

kontrolę nad swoim ekosystemem danych i umożliwić jej czerpanie wszystkich oczekiwanych korzyści gospodarczych i społecznych ze sztucznej inteligencji, konieczne jest zastosowanie kilku dźwigni.

Po pierwsze, badania i rozwój: należy dalej wzmacniać atuty Unii Europejskiej w tej dziedzinie, zwłaszcza w ramach partnerstwa publiczno-prywatnego na rzecz bezpieczeństwa cybernetycznego. Aby zebrać tak wiele pieniędzy, tego rodzaju ramy są niezbędne.

Po drugie, rozwój sektora przemysłowego wymagający zwiększonej obecności państw członkowskich i europejskich przemysłowców z branży cyfrowej w procesie certyfikacji w celu narzucenia naszych standardów i formatów danych; wymaga to również przeglądu europejskich zasad konkurencji, które muszą przyczyniać się do realizacji ambicji przemysłowych Unii, a nie je utrudniać. Komisja Spraw Europejskich Senatu szczegółowo zbadała tę kwestię. Zarówno Stany Zjednoczone, jak i Chiny wiedzą, jak radzić sobie z arsenałem publicznego wsparcia dla swoich kluczowych producentów; polityka handlowa Unii Europejskiej może tutaj również stanowić dźwignię. Unia Europejska nie powinna powstrzymywać się od rozważenia kwestii ochrony, powołując się na klauzulę bezpieczeństwa narodowego przewidzianą w art. XXI porozumień WTO, ponieważ Organ Rozstrzygania Sporów miał ostatnio możliwość potwierdzenia jej zasadności. Prezydent Stanów Zjednoczonych był bardzo zainteresowany tą koncepcją.

Wreszcie, musimy również inwestować w projekt wprowadzania sztucznej inteligencji na sposób europejski. Inwestycje w środki numeryczne przeznaczone na potrzeby sztucznej inteligencji muszą zmobilizować zarówno państwa członkowskie, jak i Unię Europejską. Chiny zamierzają zainwestować 59 mld euro do 2025 r., aby dogonić Stany Zjednoczone, które już w 2016 r. odpowiadały za 70% światowych inwestycji w sztuczną inteligencję. Unia Europejska musi również zapewnić sobie środki umożliwiające realizację jej ambicji i jest to jedno z wyzwań trwających negocjacji w sprawie jej wieloletnich ram finansowych. Francuski Senat broni potrzeby uznania sztucznej inteligencji za „projekt stanowiący przedmiot wspólnego europejskiego zainteresowania», co umożliwiłby połączenie sił europejskich graczy i zmianę biegu w kwestii narzędzi inwestycyjnych. W tym względzie wczoraj na spotkaniu z sekretarzem stanu ds. europejskich wyraziłem ubolewanie z powodu skromnych inwestycji dokonanych w tym obszarze, które stanowią zaledwie 1,11%, co jest niewystarczające z uwagi na tak wysoką stawkę.

Tylko respektując powyższe warunki będziemy w stanie zaoferować światu wiarygodny model sztucznej inteligencji, oparty na etyce ochrony danych zgodnej z naszymi wartościami: ten europejski model może stanowić przewagę komparatywną dla naszych operatorów cyfrowych, odróżniającą ich od ich chińskich, a nawet amerykańskich konkurentów. Ale ta obiecująca perspektywa będzie możliwa i wiarygodna tylko dzięki budowie prawdziwego europejskiego sektora przemysłowego opartego na sztucznej inteligencji. Wymaga to wyraźnej determinacji politycznej.

Rozpoczęła się już francusko-niemiecka współpraca na ten temat, a my skorzystalibyśmy bardzo wiele na uzupełnieniu jej współpracą z naszymi polskimi przyjaciółmi. Nasze trzy zwołane na dzisiaj zgromadzenia mogą wspólnie stanowić cenny impuls w tym kierunku. Mam nadzieję, że nasze poranne dyskusje przekonają nas do wspólnego działania w tej kluczowej dla przyszłości Unii Europejskiej kwestii.

Pozwoliłem sobie wejść w szczegóły, ponieważ temat jest bardzo obszerny. Oddaję głos mojej koleżance, Catherine Morin-Desailly, z którą dzielimy wspólną wizję tych spraw.

Catherine MORIN-DESAILLY

Senator departamentu Sekwany Nadmorskiej, przewodnicząca Komisji Kultury, Edukacji i Komunikacji

Panie Przewodniczący Komisji Spraw Europejskich, drogi Jean Bizet,

Szanowni Państwo,

Przede wszystkim chciałbym powitać naszych kolegów z Niemiec i Polski, którzy przybyli do nas w celu wspólnego zastanowienia się nad kilkoma bardzo ważnymi kwestiami. Ponadto witam również wszystkich uczestników naszego spotkania.

Dzisiejszy temat to *„Bezpieczeństwo cybernetyczne, ochrona danych i sztuczna inteligencja: jakie wyzwania dla Europy?”.* Przypominam, że nasze dzisiejsze spotkanie następuje po pierwszej konferencji, która odbyła się w Warszawie, poświęconej walce z mową nienawiści w Internecie oraz drugiej konferencji w Berlinie na temat *fałszywych wiadomości*, czyli tzw. „infox” po francusku.

Są to tematy, które bardzo dobrze znamy w Senacie, ponieważ pracujemy nad nimi już od dłuższego czasu. Poświęciliśmy im również kilka dyskusji przy okazji projektów ustaw znajdujących się w programie rządowym.

Zauważam, że pomiędzy tymi trzema tematami istnieje zarówno głęboka spójność, jak i naturalna jedność.

Jedność wyraża się poprzez pytanie o naszą cyfrową suwerenność. Bowiem to właśnie ta kwestia jest zagrożona. Wyzwaniem dla nas, w następstwie ostatnich wyborów europejskich, jest ostateczne obudzenie się i możliwość wyjścia z pewnej formy bezkrytyczności, naiwności być może, lub nawet z formy ponurej rezygnacji, która polegałaby na mówieniu sobie, że wszystko już skończone i że nie udało nam się wskoczyć do odjeżdżającego pociągu ewentualnych inwestycji w nowe technologie. Musimy natychmiast obudzić się, ponieważ staliśmy się kolonią cyfrowego świata.

Paradoksalnie, Internet narodził się po tej stronie Atlantyku, ale nie byliśmy w stanie w latach 90-tych, w przeciwieństwie do Amerykanów, inwestować w nowe technologie i pozwoliliśmy Amerykanom przejąć inicjatywę.

Jednocześnie, na drugim końcu świata, Rosjanie i Chińczycy stworzyli w tej dziedzinie swój własny ekosystem. Nadszedł zatem czas, aby wydostać się z tych kleszczy, które sytuują nas pomiędzy modelem ultraliberalnym, czasami nazywanym „kapitalizmem nadzoru”, a modelem autokratycznym na wzór tego, co jest budowane w Chinach za pomocą kredytu społecznego, z technologiami w służbie elit ustanawiających ogólny nadzór.

Uważam, że Europa, silna swoimi wartościami, może a właściwie musi opracować inny model umożliwiający przetrwanie Internetu, który jest obecnie narażony na ryzyko utraty zaufania wszystkich swoich użytkowników coraz bardziej kwestionujących jego sens z powodu aktualnej sytuacji.

Chciałbym przypomnieć, że dwa wydarzenia obudziły naszą świadomość.

Po pierwsze, sprawa Snowdena ujawniła światu system nadzoru wprowadzony przez NSA. Następnie, skandal Cambridge Analytica, ujawniony zaledwie kilka miesięcy temu, który pokazał, że wkroczyliśmy w zimną wojnę informacyjną.

Nadszedł zatem czas na reakcję, ponieważ Internet stał się rzeczywiście globalnym polem bitwy, światem hipernadzoru i bezbronności.

W Senacie, wspominał o tym Jean Bizet, od dłuższego czasu pracujemy nad rozwiązaniami, które można znaleźć we wspólnej misji informacyjnej wykonanej w 2015 r. Celem było określenie, jaki wkład może wnieść Europa w globalne zarządzanie Internetem.

Muszę podkreślić, że nasze zalecenia z tamtego okresu nic nie straciły na swojej aktualności; wprost przeciwnie wszystkie skandale pokazały konieczność pilnej reakcji.

Stwierdziliśmy, że konieczne jest opracowanie globalnej i ofensywnej strategii a Jean Bizet wyznaczył kilka jej linii. Przypomnę tutaj ich główne cechy charakterystyczne.

Po pierwsze, musimy kontynuować nasze prace nad ochroną danych. Oczywiście istnieje RODO, ale głosowanie nad nim zajęło lata, po prostu z powodu lobbingu po drugiej stronie Atlantyku, który wywierał nacisk na przywódców europejskich. Ponadto, ze względu na późne wejście w życie RODO, istnieje kilka martwych punktów. Możecie również pracować nad kwestią Internetu przedmiotów, szczególnie poprzez problematykę sztucznej inteligencji, i wiecie, że ta dziedzina przeżywa rozkwit: z tego powodu wszystkie państwa europejskie pilnie muszą zająć się kwestią certyfikacji, która gwarantuje nasze bezpieczeństwa. Dlatego też kwestia ochrony danych pozostaje sprawą najwyższej wagi.

Należy również podjąć decyzje dotyczące podatków. Jednakże, jak często podkreśla mój przyjaciel Bernard Benhamou, opodatkowanie nie może być alfą i omegą polityki na rzecz suwerenności cyfrowej. Musimy bowiem również zmienić zasady konkurencji.

Obecnie zasady konkurencji na szczeblu europejskim nie pozwalają nam na wyeksponowanie europejskich liderów w tej dziedzinie. Ponadto działają one w taki sposób, że nasze największe talenty i start-upy są stopniowo wykupywane. Krótko mówiąc, jesteśmy świadkami prawdziwego krwotoku wszystkich tych, którzy mogą pomóc nam ugruntować system cyfrowy w Europie.

Musi istnieć również możliwość zastosowania środków zabezpieczających. Czy to normalne, że skuteczne skazanie Google'a za nadużywanie pozycji dominującej zajęło aż siedem lat? Podjęte działania były z pewnością odważne i przynoszą zaszczyt pani komisarz Margrethe Vestager, ale czy zgodnie z obowiązującym prawodawstwem niemożliwe było podjęcie środków tymczasowych? W międzyczasie przedsiębiorstwa, które ucierpiały na skutek nieuczciwej konkurencji, po prostu przestały istnieć. Musimy na to zareagować, modyfikując nasze zasady konkurencji.

Należy również powrócić do dyrektywy o handlu elektronicznym. Powiedziałbym, że najlepszym sposobem walki z fałszywymi wiadomościami byłoby nadanie wreszcie statusu platformom, które dziś nie są ani dłużne, ani odpowiedzialne za nic. Moim zdaniem będzie to jeden z kolejnych projektów Komisji Europejskiej. Rząd francuski wreszcie zaczyna się nad tym zastanawiać i popierać ten pomysł. Podkreślam, że jego realizacja jest absolutnie niezbędna.

Jednocześnie Europa potrzebuje silnej polityki przemysłowej w kluczowych i strategicznych sektorach energii, zdrowia i środowiska naturalnego, ale także w dziedzinie rozwoju narzędzi kryptograficznych, które przyczynią się jutro do nowych fal uberalizacji bankowości i sektora ubezpieczeniowego.

Przede wszystkim potrzebujemy, aby wszyscy rozwijali swoje umiejętności informatyczne, ponieważ bez szkolenia, bez edukacji dla wszystkich grup wiekowych, naszych administracji i naszych polityków nie będziemy w stanie zająć się tymi wszystkimi tematami.

Musimy wspólnie posunąć do przodu całą serię kwestii, co także pociąga za sobą bardzo wysokie wymagania, jak pokazali nasi niemieccy przyjaciele w odpowiedzi na skandale Cambridge Analytica i „mafijne praktyki" na Facebooku. Nie boję się używać tego terminu, idę tutaj śladem mojego brytyjskiego odpowiednika i kolegi, Damiana Collinsa, który również używa terminu „gangster". Wykorzystując dane, Facebook doprowadził do nadużyć, jak wykazano, elementów wchodzących w zakres indywidualnej własności. W Niemczech podjęli Państwo kroki w celu zakazania agregacji danych z Facebooka, w celu zapewnienia lepszej ochrony użytkowników Internetu.

Wcale nie wierzę w możliwość wykorzystania samoregulacji, którą platformy oferują teraz z ręką na sercu jako skruchę; uważam, że należy wysunąć wysokie żądania i

postępować w sposób konsekwentny, aby zapewnić, że Internet, jeśli ma przetrwać, był regulowany prawnie.

Po drugiej stronie Atlantyku, niektórzy inżynierowie z Doliny Krzemowej, w tym jeden ze współzałożycieli Facebooka, Chris Hughes, mówią teraz o potrzebie demontażu tych platform. Rzeczywiście, stały się one rozległe i hegemoniczne, co stanowi poważne zagrożenie dla naszych demokracji, dla naszych państw. Co więcej, podważają one wszystkie środki działania publicznego, nie napotykając żadnych reakcji.

To ostatni dzwonek i musimy szybko pozbyć się pewnej formy samozadowolenia. Żałuję, że we Francji rozwija się czerwony dywan na cześć Marka Zuckerberga, który z ręką na sercu deklaruje, że platformy będą się samoregulować, ja nie wierzę w to ani przez chwilę.

Jak Państwo widzą, znajdujemy się na rozdrożu i najwyższy czas przejąć kontrolę nad naszym cyfrowym losem. Dziękuję za uwagę.

Bezpieczeństwo cybernetyczne, ochrona danych, manipulacja: porównanie sytuacji w Niemczech, Francji i Polsce

Okrągły stół moderowany przez Bernarda BENHAMOU, sekretarza generalnego Instytutu Suwerenności Cyfrowej.

W obecności:

Jean-Marie BOCKEL, senator departamentu Górny Ren, były minister, członek Komisji Spraw Zagranicznych, Obrony i Sił Zbrojnych,

Philippe BONNECARRERE, senator departamentu Tarn, członek Komisji Prawa i Komisji Spraw Europejskich,

Olivier CADIC, senator reprezentujący obywateli francuskich mieszkających poza Francją, członek Komisji Spraw Zagranicznych, Obrony i Sił Zbrojnych,

Rachel MAZUIR, senator departamentu Ain, członek Komisji Spraw Zagranicznych, Obrony i Sił Zbrojnych,

Łukasz MIKOŁAJCZYK, Senator, Wiceprzewodniczący Komisji Praw Człowieka, Praworządności i Petycji, Senat RP,

Till STEFFEN, Przewodniczący Komisji Prawnej Bundesratu, Niemcy,

Kamil BASAJ, Fundacja Bezpieczna Cybertrust, Polska,

Christian DAVIOT, Doradca ds. strategii Dyrektora Generalnego, Narodowa Agencja Bezpieczeństwa Systemów Informatycznych (ANSSI), Premier,

Frederike KALTHEUNER, Privacy International, Niemcy.

I) Uwagi wstępne

Bernard BENHAMOU

Pani Przewodnicząca,

Panie Przewodniczący,

Szanowni Państwo,

Drodzy Goście,

Z wielką przyjemnością uczestniczyłem w organizacji prac na ten tak szczególnie interesujący i niezwykle ważny dla naszych społeczeństw temat. Pani Przewodnicząca, przypomniała Pani o wyjątkowo pilnym charakterze poruszanych kwestii. Chciałbym zacytować osobę znajdującą się w tej sali, która dwadzieścia lat temu podkreślała „nieprzyjemne uczucie" odczuwane przez użytkowników, kiedy omawiane były tematy związane z bezpieczeństwem cybernetycznym.

Nie należy podchodzić do tych tematów w ten sposób. Rzeczywiście, stają się one kluczowe dla ochrony tego, kim jesteśmy, zarówno na szczeblu państw, jak i osób fizycznych, ponieważ ich celem jest ochrona naszej infrastruktury oraz uniknięcie utowarowienia danych osobowych. Oczekiwania te stanowią sedno wartości europejskich. RODO (rozporządzenie o ochronie danych osobowych) jest symbolem tego podejścia, a czasem nawet zazdrości się go nam za granicą.

Musimy jednak pójść jeszcze dalej w zarządzaniu tymi kwestiami. Wspomniane powyżej zagrożenia dotyczą wszystkich państw i zagrażają naszym demokracjom.

Niektórzy wspominali fuzję Facebooka i WhatsApp jako dowód na bezsilność Komisji Europejskiej. Chciałbym Państwu przypomnieć, że Europie udało się już w przeszłości uniemożliwić fuzję czysto amerykańskich przedsiębiorstw, takich jak General Electric i Honeywell, jeśli chodzi o turbiny lotnicze.

Do tych kwestii należy podchodzić w sposób pragmatyczny, unikając poczucia fascynacji technologicznej. Rzeczywiście, nie są to kwestie, które ograniczają się do sfery technologicznej. Stanowią one w pełni część naszego życia politycznego, zwłaszcza gdy ataki zewnętrzne mają na celu destabilizację naszych demokracji.

W obliczu tego zagrożenia konieczna jest reakcja. Ochrona danych i bezpieczeństwo cybernetyczne staną się wyznacznikami europejskimi, które mogłyby stanowić przewagą konkurencyjną, jeżeli będziemy wiedzieć, jak je wykorzystać do rozwoju naszego przemysłu technologicznego. Musimy zatem przestać myśleć o nich jako o przeszkodach w rozwoju gospodarczym.

Pani Przewodnicząca, wspomniała Pani o napięciu między modelem liberalnym, amerykańskim modelem leseferystycznym i chińskim modelem niemal dyktatorskim, gdzie każda osoba jest odnotowywana i grozi jej utrata praw socjalnych, jeżeli odbiega od „właściwej ścieżki" ustanowionej przez władze chińskie. Naszym celem musi być stworzenie trzeciej drogi, która mógłaby służyć jako podstawa do stworzenia nowego modelu ekonomicznego dla technologii.

Jednym z głównych wyzwań nadchodzących czasów dla Francji i Europy będzie zatem umożliwienie wyłonienia się tej trzeciej drogi, która szanuje zasady i wartości Europejczyków.

II) Stan zagrożeń w dziedzinie bezpieczeństwa cybernetycznego

Bernard BENHAMOU

Rozpoczniemy nasz pierwszy okrągły stół przeglądem ryzyka związanego z bezpieczeństwem cybernetycznym. Rozpocznijmy naszą podróż od analizy Christiana Daviot doradcy w ANSSI.

Christian DAVIOT

Chciałbym zaznaczyć, że wypowiadam się tutaj we własnym imieniu, a nie jako przedstawiciel ANSSI.

Wszyscy znamy naturę istniejących zagrożeń. Bardzo dużo się dyskutuje na ich temat. Chciałbym wspomnieć o znacznie bardziej niebezpiecznym politycznym zagrożeniu występującym w trzech reprezentowanych dziś tutaj krajach. Hannah Arendt napisała, że w próżnię myśli wpisano zło. Wydaje mi się, że należy pilnie zastanowić się nad definicją pewnych pojęć w świetle prawa międzynarodowego. ONZ podkreśliło, że prawo międzynarodowe ma zastosowanie do przestrzeni cyfrowej. Nie istnieje jednak żadna definicja tego terytorium. Europa nie może obejść się bez zastanowienia się nad tą kwestią, która jest niezbędnym warunkiem wstępnym dla określenia trzeciej drogi.

Moim zdaniem zagrożenie polega na tym, że terminy te nie są definiowane. W tym celu parlamentarzyści i wszystkie podmioty społeczeństwa obywatelskiego muszą współpracować z ekspertami, by omówić te pojęcia i ustalić jasne definicje. Największe niebezpieczeństwo polega na tym, że obecnie nikt nad tym nie pracuje.

Bernard BENHAMOU

Przyjrzyjmy się teraz, jak te same zagrożenia są postrzegane w Niemczech.

Till STEFFEN

Zagrożenia te wynikają z różnorodnych przyczyn, a ryzyko polega na wzięciu pod uwagę tylko niektórych z nich. Ktoś wspomniał o dużych grupach, takich jak Facebook, który czasami musi być traktowany jako organizacja o metodach przestępczych ze względu na swoją siłę ekonomiczną. W związku z tym wydaje mi się absolutnie konieczne, abyśmy mogli dzisiaj o tym podyskutować.

Bernard BENHAMOU

Pozjnajmy teraz punkt widzenia naszych polskich sąsiadów w kwestiach bezpieczeństwa cybernetycznego i ochrony danych.

Łukasz MIKOŁAJCZYK

To bardzo ważny temat. Liczba ataków cybernetycznych będzie rosła wraz z wzrostem zagrożeń. W naszym codziennym życiu, obywateli, administracji i przedsiębiorstw, rzeczywistość wirtualna odgrywa coraz ważniejszą rolę, zwiększając tym samym ryzyko ataków i manipulacji.

Kolejnym zagrożeniem jest wzrost zdolności operacyjnych organizacji terrorystycznych. Dlatego też naszym priorytetem musi być wzmocnienie krajowych zdolności reagowania. Przy właściwym ministerstwie w Polsce powołano grupę roboczą, przeprowadzono odpowiednie szkolenia na temat dezinformacji. Poza tym stworzyliśmy stronę internetową, na której informujemy obywateli o tych kwestiach.

III) Podnoszenie świadomości użytkowników w zakresie zagrożeń dla bezpieczeństwa cybernetycznego

Bernard BENHAMOU

W jakim stopniu środki polityczne mogą jak najlepiej wspierać użytkowników?

Philippe BONNECARRERE

Aktualnie, wydaje mi się, że obywatele nie są wystarczająco świadomi powyższych kwestii. Sytuacja przypomina wyścig pomiędzy rozwojem cyfrowym z jednej strony, a multiplikacją połączonych obiektów i sieci z drugiej strony.

Opóźnienie naszej reakcji jest tym bardziej niebezpieczne, że ryzyko nie jest fizyczne. W świecie cyfrowym nie dostrzegamy zagrożenia, co jeszcze bardziej utrudnia podnoszenie poziomu świadomości.

We Francji nasze podejście do tych tematów ograniczało się dotychczas do sfery prawnej. Doprowadziło to do ustanowienia RODO, które zostało następnie uzupełnione środkami na poziomie krajowym. Ten arsenał tekstów jest z pewnością konieczny, ale nie stanowi wystarczającej odpowiedzi.

Moim zdaniem musimy wygrać bitwę o kulturę cyfrową. Mimo wszystko odnotowałem kilka obiecujących elementów. Na przykład, opcja cyfrowa zostanie wdrożona w przyszłym roku w ramach matury. Nauczyciele nadal muszą być szkoleni w tym nowym wymiarze nauczania.

Tej kultury należy uczyć od najmłodszych lat. Mój ośmioletni wnuk opanował techniczny aspekt telefonu komórkowego, ale nie posiada żadnej wiedzy na temat bezpieczeństwa cyfrowego. Umiejętność posługiwania się technologiami cyfrowymi należy zatem rozumieć zarówno z technicznego punktu widzenia, jak i pod kątem kwestii bezpieczeństwa.

Bernard BENHAMOU

Jakie środki wsparcia dla obywateli zostały przyjęte w Niemczech?

Frederike KALTHEUNER

Chciałabym podkreślić, że użytkownik jest tutaj najsłabszym ogniwem. Dlatego też nie chodzi o obarczanie go odpowiedzialnością za problemy związane z bezpieczeństwem. W grudniu 2018 r. przeanalizowaliśmy najpopularniejszą aplikację mobilną z dziesięcioma milionami użytkowników. Pod koniec badania okazało się, że ponad 60 % danych zostało udostępnionych innym podmiotom, co stoi w całkowitej sprzeczności z RODO.

Ten przykład dowodzi rozbieżności między tym, co pokazuje Unia Europejska, a rzeczywistością faktów. Ponadto kwestie te są ściśle związane z pojęciem sprawiedliwości społecznej. Rzeczywiście, wielu użytkowników nie może inwestować w urządzenia wysokiej klasy. Opierając się na tanim sprzęcie, narażają się na ryzyko działania smartfonów z większą ilością naruszeń i braków dotyczących bezpieczeństwa.

Ogólnie rzecz biorąc, problemy te w dużej mierze wykraczają poza świadomość obywateli.

Bernard BENHAMOU

Kwestie te muszą być rzeczywiście omówione ze wszystkimi krajowymi organami regulacyjnymi. Jak wygląda wsparcie oferowane w Polsce?

Kamil BASAJ

Potrzeba edukacji nigdy nie będzie mogła zostać w pełni zaspokojona. Świat cyfrowy staje się coraz bardziej złożony tak szybko, że poziom kompetencji wymaganych do jego opanowania stale rośnie. Na przykład coraz częstsze korzystanie z połączonych systemów wiąże się ze szkoleniem obywateli w zakresie zagrożeń związanych z wykorzystaniem tych narzędzi w złej wierze. Państwo musi w pełni przyjąć na siebie odpowiedzialność w obliczu tych nowych zagrożeń.

Ponieważ jednak bezpieczeństwo cybernetyczne ma wymiar transgraniczny, działania muszą być prowadzone wspólnie. Podobnie, istnieje potrzeba dalszego ostrzegania użytkowników o tych kwestiach.

IV) Przygotowanie państw europejskich na zagrożenia dla bezpieczeństwa cybernetycznego

Bernard BENHAMOU

Dziękuję za zwrócenie uwagi, że potencjał ataku jest jeszcze w powijakach i że jego rozwój wydaje się nieuchronny wraz z rozwojem obiektów połączonych. Jest to okazja do zastanowienia się nad zdolnościami państw europejskich do sprostania tym wyzwaniom. Jak wyglądają możliwości zmian legislacyjnych w celu uregulowania tych kwestii?

Zauważyłem również, że stwarzają one realne problemy dla suwerenności państwa; aby zilustrować mój punkt widzenia, chciałbym wspomnieć w szczególności o wprowadzeniu nowej waluty na Facebooku, czyli Libry. Stworzenie waluty przez prywatnego operatora rodzi wiele pytań.

Co o tym sądzisz, Rachel Mazuir?

Rachel MAZUIR

Zauważyłam, że wszyscy podzielamy wątpliwości i nadzieje dotyczące tych kwestii. We Francji potrzebę zajęcia się tymi sprawami potwierdzono w 2008 r. w *Białej księdze obrony*

narodowej, a następnie w 2017 r. ANSSI została utworzona w 2009 r. Agencja ta cieszy się międzynarodowym uznaniem, a jej działalność stale się rozwija.

Ponadto Francja posiada solidne ramy prawne i regulacyjne, szczególnie w sektorze elektronicznym. W związku z tym, operatorzy telekomunikacyjni mają obowiązek pomagać w wykrywaniu ataków.

Uruchomienie 5G rodzi nowe pytania. W celu lepszej ochrony bezpieczeństwa cyfrowego, projekt ustawy zostanie przedłożony parlamentarzystom w ciągu kilku dni. Zawiera on także zupełnie nowe dyspozycje na poziomie międzynarodowym.

Poza tym, wydaje mi się, że konieczne jest zapewnienie ochrony wzajemnie połączonych sieci. Ponieważ poziom bezpieczeństwa cybernetycznego w Europie jest bezpośrednio związany z poziomem bezpieczeństwa każdego państwa, dlatego też konieczne jest zapewnienie Europie wspólnych standardów i celów, aby zapewnić solidne podstawy bezpieczeństwa cybernetycznego we wszystkich państwach członkowskich.

Na zakończenie zacytuję: *„Najlepszy dowódca to ten, który przygotowuje wojnę i wygrywa ją bez konieczności jej prowadzenia."*

Christian DAVIOT

Chciałbym zwrócić uwagę, że zdolności ofensywne i obronne są ściśle rozdzielone w naszym francuskim modelu. ANSSI jest więc agencją pełniącą jedynie rolę obronną.

Bernard BENHAMOU

Poznajmy teraz na punkt widzenia Niemiec.

Till STEFFEN

Przypomniano już wiele istotnych elementów. Chciałbym poruszyć kwestię istotną dla Europy. Ponieważ państwa członkowskie opierają się na systemach demokratycznych, zależą one od zaufania, jakim obdarzają je ich obywatele. Jednak organizowane z zagranicy kampanie dezinformacyjne próbują zdestabilizować nasze państwa. Na przykład roboty tworzące fałszywe konta na forach lub portalach społecznościowych mają na celu przekonanie ludzi, że wyrażane są pewne opinie. Musimy być tego świadomi, ponieważ takie sytuacje są bardzo niebezpieczne dla naszych demokracji. W Niemczech odnotowaliśmy kilka takich działań z Rosji. Należy pilnie chronić się przed tymi zjawiskami.

W obliczu tych zagrożeń nasze demokratyczne debaty zbyt często ograniczają się do sfery krajowej, zwłaszcza ze względu na barierę języka. Ryzyko związane z tym podziałem polega na postrzeganiu tylko części debat w państwach sąsiadujących. To otwiera drzwi dla tych, którzy mają złe zamiary wobec nas.

Wszystkie wymienione tu zalecenia mogą zostać wdrożone tylko wtedy, gdy utrzymane zostanie demokratyczne podejście do tych kwestii. Musimy wzmocnić dialog między nami i przeprowadzać kampanie uświadamiające.

Ponadto musimy zastanowić się nad naszą zdolnością reagowania na te szczególnie dobrze ukierunkowane kampanie, które są źródłem wielu debat publicznych. Komisja Europejska musi zatem wyposażyć się w odpowiednie narzędzia do radzenia sobie z takimi sytuacjami.

Bernard BENHAMOU

W tym względzie chciałbym przypomnieć, że tylko w pierwszym kwartale 2018 r. Facebook usunął 583 miliony fałszywych kont, czyli jedną czwartą wszystkich aktywnych kont. Rzeczywiście, te fałszywe rachunki były wykorzystywane do wpływania na opinię publiczną. W tej skali to już nie rzemiosło, ale przemysł ciężki pod względem manipulacji mas. Jak wygląda stanowisko Polski w tej sprawie?

Łukasz MIKOŁAJCZYK

Kiedy mówimy o bezpieczeństwie cybernetycznym, nie możemy mieć nadziei na osiągnięcie całkowitego bezpieczeństwa. Konieczne jest przyjęcie zdecydowanych środków postępowania w przypadku ataków, co oznacza dostosowanie prawodawstwa do zmieniającego się otoczenia. Każde państwo zależy oczywiście od własnej infrastruktury, ale zależy też od infrastruktury międzynarodowej.

Stopniowo budujemy system rozwijający nasze zdolności reagowania, ale cały czas trwa wyścig między zagrożeniami a naszymi odpowiedziami na nie. Aktualnie wszystkie sektory gospodarki są bardzo podatne na zagrożenia. Konieczne jest zatem rozwijanie naszych zdolności do ich zwalczania.

V) Pożądane podejście Europy do zagadnienia 5G

Bernard BENHAMOU

Zajmiemy się kwestią, która spowodowała wiele napięć między Stanami Zjednoczonymi i Chinami. Chodzi o firmę Huawei, której produkty zostały oskarżone o dobrowolne wprowadzenie przez producenta naruszeń bezpieczeństwa. Jaki powinien być nasz stosunek do tego typu sytuacji, biorąc pod uwagę, że 5G znajduje się obecnie w fazie rozmieszczania?

Jean-Marie BOCKEL.

Myślę, że istotne jest poruszenie tego tematu w kontekście tej wspólnej pracy Niemiec i Polski. Byłem na posiedzeniu Zgromadzenia Parlamentarnego NATO, gdzie przedstawiłem sprawozdanie na temat kwestii cyfrowych i obrony cybernetycznej. Wspomniano o sprawie firmy Huawei. To pytanie nie jest nowe.

Ja sam bardzo ostrożne podchodziłem do tego chińskiego giganta w oparciu o francuską doktrynę, która rozwinęła się na przestrzeni lat. Wzywa ona do zachowania ostrożności i czujności w obliczu niebezpieczeństwa funkcjonowania niektórych produktów jak koń trojański. Konieczne jest zatem znalezienie właściwej równowagi między czysto naiwną postawą i jej nadmiernie negatywnym przeciwieństwem. W tym kontekście uznaliśmy, że Huawei może się rozwijać pod pewnymi warunkami. Ze swej strony Wielka Brytania poszła w ślad za Amerykanami decydując się całkowicie zakazać sprzedaży. Niemcy również przyjęły wyważone stanowisko. Wydaje mi się, że tak samo jest w Polsce.

Co powinna zrobić Europa w tym geopolitycznym kontekście w stosunku do niektórych zakazów? To pytanie rodzi kolejne: co z *„dealem”*, aby użyć wyrażenia Prezydenta Donalda Trumpa? W ramach trwających negocjacji handlowych między Chinami a Stanami Zjednoczonymi ogłoszono *deal*. Powstaje zatem pytanie, czy Huawei będzie jego częścią.

Wiem, że ANSSI zadaje sobie te same pytania. Czy powinniśmy przyjąć wizję identyczną z wizją Amerykanów, czy też opracować własne podejście? W drugim przypadku kwestią tą należy się oczywiście zająć na szczeblu europejskim. Na własną rękę nie bylibyśmy w stanie zrobić tego w stosunku do takich gigantów jak Stany Zjednoczone czy Chiny.

Bernard BENHAMOU

W tych bardzo technicznych kwestiach interesuje nas opinia ekspertów ds. bezpieczeństwa. Dlatego oddaję głos Christianowi Daviot.

Christian DAVIOT

We Francji toczy się obecnie dyskusja nad ustawą. Osobiście zauważyłem, że stanowiska przyjęte w Wielkiej Brytanii, Niemczech i Francji są bardziej ogólne, ponieważ nie dotyczą konkretnego producenta.

Ogólnie rzecz biorąc, musimy zachować czujność w odniesieniu do tego sprzętu. W przypadku sprawy Snowdena, został w nią zamieszany amerykański producent. Pokazuje to wyraźnie, że nie możemy pokładać ślepego zaufania w żadnym przedsiębiorstwie.

Bernard BENHAMOU

Jakie jest stanowisko Niemiec w tej sprawie?

Till STEFFEN

Moim zdaniem podejście rządu niemieckiego nie jest wystarczająco twarde. Pozostaje ostrożny, co powoduje pewne niespójności w podejmowanych działaniach. Zdecydowaliśmy się zezwolić na wdrożenie 5G, o ile nie będziemy zależni od produktów Huawei.

Jednakże, nie posuwając się do stwierdzenia, że tylko produkty europejskie są dopuszczone w Europie, powinniśmy nadal zapewniać europejską alternatywę w dziedzinie infrastruktury. Odpowiedź ta musi być na tym samym poziomie, co w przykładzie Airbusa. Dla przypomnienia, kiedy powstawał Airbus, istniał również problem monopolu dla Boeinga.

Musimy zatem wspierać tego rodzaju podejście, które oczywiście obejmuje odpowiednie umiejętności i zasoby, ale także współpracę pomiędzy agencjami europejskimi i krajowymi.

Dzięki połączeniu naszych wysiłków możliwe będzie wyposażenie się w odpowiednie środki do rozwiązywania tych problemów.

Bernard BENHAMOU

W tym względzie Francja i Niemcy zdecydowały się na współpracę w celu opracowania europejskiej alternatywy. W przeciwnym razie doprowadziłoby to do zwiększenia podatności Europy na zagrożenia. A co z Polską?

Łukasz MIKOŁAJCZYK

Oczywiście, Polska podziela określony tutaj cel bezpieczeństwa. Obecnie znajdujemy się w fazie konsultacji z operatorami telekomunikacyjnymi, którzy są pełnoprawnymi partnerami. Należy w pełni zająć się kwestią wdrożenia 5G, ponieważ 5G będzie ostatecznie pilotować wszystkie systemy i przyspieszy rozwój cyfrowy.

Podzielam pogląd, że Europa mus dać wspólną odpowiedź.

Frederike KALTHEUNER

Pytanie to odnosi się do kwestii dominacji USA i Chin i wymaga przede wszystkim określenia, jakie innowacje są pożądane, a nie na ograniczeniu ich do problemów konkurencji.

Osobiście chciałabym ponownie skupić się na prawach jednostki, które są najbardziej narażone na te zagrożenia. Unia Europejska musi dążyć do opracowania strategii bardziej zorientowanej na ochronę danych. W związku z tym nie może ona zmierzać w kierunku modeli amerykańskich i chińskich ograniczających się do aspektów konkurencyjnych.

VI) Europejskie zdolności ofensywne w zakresie potencjalnych wojen cybernetycznych

Bernard BENHAMOU

Pojawia się również kwestia potencjalnej wojny opartej na ataku na naszą infrastrukturę cyfrową. W tym kontekście skupmy się na naszych zdolnościach

ofensywnych. Rzeczywiście, w pewnym momencie opór staje się niewystarczającą strategią i musi zostać uzupełniony działaniami ofensywnymi. Wysłuchajmy zdania Oliviera Cadic na ten temat.

Olivier CADIC

Po pierwsze, chciałbym powiedzieć, że obecnie toczy się wojna. Przykro mi, ale musimy zdać sobie sprawę, że czasy się zmieniły. Ostatnie oficjalne wypowiedzenie wojny przez państwo europejskie to rok 1982 r.: Wielka Brytania przeciwko Argentynie. Niemniej, Rosjanie codziennie testują nasze systemy obronne. Na przykład, próbowali zakłócić nasze systemy komunikacyjne w marynarce wojennej.

Ze swej strony Chiny wyraźnie stwierdziły, że ich celem jest zdominowanie świata do 2050 r. i uważają, że nasze systemy demokratyczne są przestarzałe. Z drugiej strony, Amerykanie postrzegają świat jako terytorium, które muszą dominować z punktu widzenia gospodarki.

Poza państwami istnieją organizacje przestępcze i grupy terrorystyczne celujące w reputację demokracji. Czasami cel jest tak istotny jak w niedawnym ataku na nasze systemy zaopatrzenia w wodę.

Mówiłem, że wasza teraźniejszość to nasza przeszłość. Kiedy komentujemy wiadomości, jest już po wszystkim. Tak więc, o Librze mówiono w tym tygodniu, mimo że Facebook rozwija projekt tej waluty od wielu lat. To pokazuje, że ciągle jesteśmy spóźnieni.

W obliczu tych wyzwań, stworzenie zdolności ofensywnych to minimum, jakie możemy zrobić. Minister obrony ogłosił na początku roku, że Francja wyposaży się w środki ofensywne. Techniki te zostały już wykorzystane przeciwko Daechowi.

Na celowniku jest serce naszego systemu. Wystarczy wspomnieć trolle atakujące konto prezydenta Republiki na Twitterze. Od lat wzywam do wdrożenia elektronicznej szczepionki, aby przeciwdziałać tego typu działaniom.

W rezultacie stoimy w obliczu wyzwań, którym nie jesteśmy w stanie sprostać sami. Jedynym rozwiązaniem jest zatem połączenie sił wszystkich państw członkowskich, co oznacza wcześniejsze określenie priorytetów.

Bernard BENHAMOU

Jest to rzeczywiście delikatny temat. A co z niemiecką doktryną na ten temat?

Till STEFFEN

To, co zostało powiedziane, zgadza się. Mamy do czynienia z o wiele bardziej niebezpiecznymi sytuacjami niż w przypadku tradycyjnych wojen. Za czasów mojej młodości we Frankfurcie było kilka scenariuszy odpowiedzi na ewentualny atak rosyjskich czołgów.

Aktualne zagrożenia związane z atakiem internetowym mogą spowodować znacznie większe szkody. Pokazuje to przykład ataku na system wodociągowy.

Ponadto zagrożenie może pochodzić od organizacji przestępczej, grupy terrorystycznej lub poszczególnych osób. Pozostaję jednak ostrożny, kiedy mówimy o strategii kontrataku. Z pewnością możliwe jest odpieranie codziennych ataków, których są miliony, ale jeśli zdecydujemy się na działania odwetowe, w jaki sposób zidentyfikujemy cel? Jak możesz być pewny, że dobrze celujesz? W rzeczywistości nadal istnieją wątpliwości co do pochodzenia ataku, co oznacza zachowanie czujności wobec ryzyka wystąpienia niebezpiecznego efektu domina.

Olivier CADIC

Zaletą posiadania środków ofensywnych jest to, że strona przeciwna również czuje się zagrożona. Ponadto, jeśli ograniczymy się tylko do systemu czysto obronnego, istnieje ryzyko, że on już nie zadziała.

Przykład Huawei mówi sam za siebie: zaakceptowaliśmy wprowadzanie do obrotu produktów tej firmy, chociaż Chiny nie rewanżują się. Moim zdaniem to podejście samobójcze pokazujące, że model chiński jest problematyczny. Zadaję pytanie: kiedy zdecydujemy się zmienić nasze zachowanie?

Jean-Marie BOCKEL

Możliwości ofensywne Francji są nowe. Znaczący postęp polega na tym, że obecnie istnieje doktryna dotycząca ich użycia. Jakiś czas temu dowiedziałem się o systemach ofensywnych w sposób poufny. Poufność związana z tymi technikami nie wydawała mi się problematyczna, brakowało mi natomiast doktryny dotyczącej ich użycia.

Ponadto techniki odstraszają tylko wtedy, gdy towarzyszą im rzeczywiste działania. Cieszę się, że przeszliśmy od „działania bez mówienia” do „działania informując o tym”.

Jest jeden czuły punkt dotyczący skali systemów ofensywnych. Moim zdaniem dziedzina ta nadaje się bardziej do współpracy dwustronnej niż do stania się częścią szerszego systemu. Im więcej państw angażuje się w tego typu działania, tym bardziej słabe punkty każdego z nich narażone są się narażone na zagrożenia.

Polityka obronna musi zatem przede wszystkim umożliwić wzmocnienie każdego z nich. Oznacza to pogodzenie suwerenności narodowej ze wspólnym działaniem.

Bernard BENHAMOU

Jak Polska radzi sobie z tymi tematami?

Łukasz MIKOŁAJCZYK

Jest to rzeczywiście delikatny temat i Polska potraktowała go jako taki. W pełni zgadzam się z poprzednimi uwagami. Musimy działać razem na szczeblu krajowym i międzynarodowym. Ponadto należy stworzyć warunki do współpracy między platformami internetowymi a sferą społeczną. Będzie się to wiązało z ustanowieniem partnerstw publiczno-prywatnych, które uniemożliwią jakiekolwiek działania dezinformacyjne. W ostatecznym rozrachunku poprawi to bezpieczeństwo.

VII) Rola Unii Europejskiej w dziedzinie bezpieczeństwa cybernetycznego

Bernard BENHAMOU

Przejdziemy do ostatniej części naszego pierwszego okrągłego stołu. Na czym mogłaby polegać rola Unii Europejskiej w dziedzinie bezpieczeństwa cybernetycznego? To pytanie jest przedmiotem wielu debat. Co o tym myśli Philippe Bonnecarrère?

Philippe BONNECARRERE

Wszyscy mamy nadzieję, że Unia Europejska będzie mogła w pełni odegrać zamierzoną rolę w tej kwestii. Rzeczywiście, zagrożenie nie jest ograniczone terytorialnie. Wszystkie nasze państwa są przepuszczalne i współzależne. Nieskuteczne byłoby zatem zajmowanie się tym tematem wyłącznie na szczeblu krajowym.

Mamy pewne przepisy regulacyjne, takie jak RODO. Podobnie Unia Europejska ustanowiła agencję, której stopniowo nabiera coraz większego znaczenia: Enisa.

Niemniej jednak Unia Europejska musi rozwijać swoje działania na planie kulturowym wprowadzając automatyzmy bezpieczeństwa wśród obywateli. Konieczne jest wypracowanie odpowiednich reakcji na zagrożenia cyfrowe.

Dlatego wydaje mi się, że nasza walka musi polegać na przejściu od czysto prawnej reakcji do reakcji globalnej. Oczywiście, ta ewolucja wymaga czasu.

Bernard BENHAMOU

Jak wygląda stanowisko Niemiec w tej sprawie? Jakie istnieją zalecenia?

Till STEFFEN

W moim podejściu do tematu zawsze staram się uwzględniać wymiar europejski. To pytanie zadawane jest nam wszystkim jako decydentom politycznym. Ważne jest, abyśmy przezwyciężali nasze różnice polityczne, a nie je pogłębiali. Tylko razem, a nie przeciwko sobie, możemy sprostać tym nowym wyzwaniom.

To wspólne podejście musi mieć również zastosowanie w kwestiach regulacji. Jeśli chodzi o RODO, Niemcy przyhamowały Francję, jeśli chodzi o współpracę między różnymi agencjami bezpieczeństwa. Ten rodzaj zachowania musi być zwalczany. Wszyscy musimy podejmować wysiłki, ryzykując, że nie będziemy w stanie rozwiązać tych problemów.

Bernard BENHAMOU

Dziękuję za szczerość. Ostatnie słowo Łukasza Mikołajczyka na temat europejskiego działania.

Łukasz MIKOŁAJCZYK

Ponieważ Unia Europejska dysponuje ogromnym potencjałem technicznym, naukowym i ludzkim, należy z niego korzystać. Wszystko, co zostało powiedziane, jest słuszne, musimy współpracować w tych kwestiach na szczeblu europejskim. W tym celu konieczne jest poszukiwanie konsensusu, który umożliwi znalezienie wspólnych rozwiązań w Unii Europejskiej. Należy również zintensyfikować działania przedsiębiorstw i nadać im wymiar europejski.

Sztuczna inteligencja: jakie kwestie etyczne, przemysłowe i polityczne?

Okrągły stół moderowany przez Bernarda BENHAMOU, sekretarza generalnego Instytutu Suwerenności Cyfrowej.

W obecności:

André GATTOLIN, senator departamentu Hauts-de-Seine, członek Komisji Spraw Europejskich, autor raportu informacyjnego na temat „Europejskiej strategii na rzecz sztucznej inteligencji".

Gérard LONGUET, senator departamentu Moza, były minister, przewodniczący parlamentarnego Biura ds. Oceny Wyborów Naukowych i Technologicznych, sprawozdawca senackiej Komisji Śledczej ds. Suwerenności Cyfrowej.

Konstanty RADZIWIŁŁ, Senator, były minister, Senat RP

Till STEFFEN, Przewodniczący Komisji Prawnej Bundesratu, Niemcy

Anthony COLOMBANI, Francuska Federacja Telekomunikacyjna

Wojciech ORLIŃSKI, polski dziennikarz

I) Potrzeba ustanowienia strategii etycznej charakterystycznej dla Europy

Bernard BENHAMOU

Trzeba powiedzieć, że Europa nie zajmuje obecnie miejsca, które powinna zajmować w dziedzinie sztucznej inteligencji. Niektórzy z was pracowali zresztą nad tym zagadnieniem.

Fakt, że najlepsze europejskie mózgi odchodzą do pracy w firmach amerykańskich lub chińskich nie stanowi powodu do zadowolenia. Kwestia ta jest równie istotna dla opinii publicznej. Sztuczna inteligencja będzie odgrywać rolę we wszystkich sektorach gospodarczych i społecznych, co oznacza, że należy umieścić ją w centrum naszych politycznych refleksji.

Zaczniemy od André Gattolin. Co sądzisz o działaniach i polityce publicznej w tym obszarze? Jak daleko powinniśmy się posunąć? Odbyło się już kilka debat na temat bioetyki. Czy to samo powinno być zrobione w kwestii sztucznej inteligencji?

André GATTOLIN

Chyba tak. Prace Cédrica Villaniego podkreślają znaczenie zdefiniowania etyki w dziedzinie sztucznej inteligencji. To wydaje mi się niezbędne. Komisja Europejska zaczęła stosować swój plan działań w tym zakresie, aby odzwierciedlić szczególną wizję Europy w tym zakresie i dostosować ją do naszego demokratycznego modelu.

My, Europejczycy, mamy teorię prawną opartą na filozoficznej i politycznej konstrukcji naszego kontynentu. Powoduje ona, że zwracamy szczególną uwagę zarówno na poszanowanie wolności jednostki, jak i praw ludów i narodów. W tym kontekście świat sztucznej inteligencji musi być w stanie zagwarantować poszanowanie wszystkich tych swobód.

Niemniej jednak wydaje mi się, że nie powinniśmy wprowadzać zbyt restrykcyjnego prawodawstwa, które ograniczałoby rozwój sztucznej inteligencji w dziedzinie gospodarki. Dlatego też nasze podejście musi być zrównoważone.

II) Ustanowienie demokratycznej debaty na temat kwestii związanych ze sztuczną inteligencją

Bernard BENHAMOU

Jesteśmy świadkami szybkiego wzrostu liczby inteligentnych asystentów cyfrowych, które stwarzają nowe zagrożenia dla ich użytkowników. Na dzień dzisiejszy 20% Amerykanów posiada takie urządzenie. W tym kontekście, co sądzicie o potrzebie demokratycznej debaty na ten temat? Czy byłoby to przydatne?

Till STEFFEN

Zgadzam się. Potrzebujemy publicznej debaty. Obserwuję obecnie spore pomieszanie w opinii publicznej, jeśli chodzi o te kwestie. To wydaje mi się bardzo ryzykowne. W mojej partii jest grupa robocza zajmująca się programami komputerowymi. Jeden z ekspertów zauważył, że pojęcie sztucznej inteligencji zastąpiło pojęcie oprogramowania; pułapką byłoby zakwalifikowanie jako sztucznej inteligencji każdego trudnego do zrozumienia oprogramowania oraz używanie w debacie publicznej słów kluczowych nieodpowiednich do sytuacji. Mam wrażeni, że nikt już nie rozumie, o czym mówimy.

Ponadto musimy wziąć na siebie odpowiedzialność w odniesieniu do produktów wprowadzanych do obrotu. Konieczna jest również większa przejrzystość w odniesieniu do usług związanych z tymi nowymi narzędziami.

Debaty na temat ram regulacyjnych z jednej strony, a etyki z drugiej strony, należy wyraźnie rozróżnić. Jednak do tej pory odbyła się tylko debata na temat regulacji, nad czym ubolewam.

Bernard BENHAMOU

Jakie byłyby w tym przypadku obszary wymagające poprawy? Panie Ministrze, co pan o tym sądzi?

Gérard LONGUET

Po pierwsze, chciałbym podkreślić, że parlament francuski jest w stanie sporządzić opis aktualnej sytuacji w tej dziedzinie i udowodniał to zawsze, gdy tylko Senat i Zgromadzenie Narodowe wyraziły taką potrzebę.

Musimy znaleźć wiarygodną drogę pomiędzy dwoma biegunowymi stanowiskami, z którymi zbyt często się spotykamy: z jednej strony - uznawanie sztucznej inteligencji jako środka pozbawiania człowieka jego autonomii; z drugiej strony - pomniejszenie jej znaczenia i sprowadzenie jej do zwykłego systemu. Z jednej strony jest to scenariusz apokaliptyczny, z drugiej strony mamy tendencję do trywializowania sztucznej inteligencji. Musimy zatem znaleźć właściwą równowagę między tymi dwiema drogami.

Zawsze bardzo podziwiałem niemiecką demokrację opierającą się na zasadach decentralizacji i reprezentacji proporcjonalnej. We Francji te dwie zasady są dla nas całkowicie obce. Niestety, prowadzi to do tego, że obywatele rezygnują z indywidualnej odpowiedzialności za udział w debacie publicznej. Stopniowo, jedyne omawiane kwestie publiczne sprowadzają się do zainteresowania nazwiskiem kolejnego polityka.

Debaty na temat sztucznej inteligencji odsunęły się ze sfery politycznej nie z powodu ich trudności, ale raczej z powodu postrzegania, że decyzje w tej sprawie należą do władzy wykonawczej.

Bernard BENHAMOU

Być może systemy sztucznej inteligencji mogłyby zmienić debaty ze względu na nowe perspektywy oddziaływania na ludność.

Gérard LONGUET

W tym względzie chciałbym poczynić uwagę: analiza wyborców nie jest nowa. Innowacyjność polega na zdolności do dostarczania bardziej szczegółowych informacji.

Bernard BENHAMOU

A co z tym tematem w Polsce?

Konstanty RADZIWIŁŁ

Ta debata jest pasjonująca, ale znacznie bardziej złożona niż pierwszy okrągły stół. Zawiera ona bowiem główne pytania dotyczące naszej przyszłości, które muszą być rozpatrywane z dużą dozą pedagogiki. Opinia publiczna często myśli, że roboty zwracają się przeciwko ludziom, uciekając spod ich kontroli.

Ta karykaturalna wizja musi być zwalczana. Narzędzie, jakie stanowi sztuczna inteligencja, musi być lepiej rozumiane. Musimy oczywiście ostrzegać nasze społeczeństwa przed niektórymi formami sztucznej inteligencji, aby obywatele byli świadomi pewnych zagrożeń.

Jednak sztuczna inteligencja może zapewnić nam niewiarygodne korzyści, szczególnie w zakresie zdrowia. To samo dotyczy autonomicznych samochodów lub zarządzania miastami. Narzędzia te nie powinny być jednak brane pod uwagę jako zwykłe produkty. Unia Europejska próbuje ustanowić ramy w dyrektywie w sprawie odpowiedzialności ponoszonej z powodu produktów, ale to dopiero początek.

Umieszczone w niewłaściwych rękach, narzędzie to może zostać przekształcone w broń, zarówno indywidualną, jak i masowej destrukcji. To sprawia, że narzędzie to musi być traktowane z należytą ostrożnością, tak samo jak w przypadku niektórych wrażliwych sektorów gospodarki, np. branży jądrowej.

III) Perspektywa definicji etycznej właściwej dla Europy

Bernard BENHAMOU

Kontynuujemy na temat kwestii etycznych. Co Europa mogłaby zrobić, aby stworzyć swoją własną drogę? Anthony Colombani pracujący w sektorze telekomunikacji może na pewno powiedzieć nam coś na ten temat.

Anthony COLOMBANI

Jeśli chodzi o potrzebę wyboru ścieżki pośredniej, Europa może i powinna to zrobić. Zaczęła już wprowadzać w życie doskonałe wytyczne w tym zakresie, takie jak przepisy zakazujące stosowania autonomicznej broni śmiercionośnej. Należy przyznać, że uregulowanie kwestii prywatności będzie skutkowało ograniczonym postępem.

Niemniej jednak etyka musi być postrzegana jako warunek społecznej akceptacji sztucznej inteligencji, a nie jako bariera. Inaczej to nie zadziała. Jeśli ludność uświadomi sobie, że sztuczna inteligencja narusza prywatność, będzie się jej sprzeciwiać. Ramy etyczne są zatem absolutnie niezbędne dla rozwoju tej branży. To wyzwanie cywilizacyjne, które przed nami stoi. Ponadto pytania filozoficzne stanowią integralną część badań prowadzonych obecnie przez bardzo wysoko wykwalifikowanych programistów.

Bernard BENHAMOU

Przejdźmy teraz do niemieckiej wizji w tej sprawie.

Leonie BEINING

Zgadzam się również z kierunkami, jakie obecnie obrała Unia Europejska. Musimy pamiętać, że technologie są zglobalizowane. W związku z tym poszczególne kraje rozwijają własną politykę, a Europa musi stworzyć swoją własną. W szczególności niezbędne wydaje się podjęcie decyzji o sposobie transpozycji norm w państwach członkowskich.

Chciałbym wspomnieć o przypadku Chin, które oficjalnie przyjęły zasady ochrony prywatności, chociaż w rzeczywistości wszyscy wiemy, że nie są one tam stosowane.

Bernard BENHAMOU

Przejdźmy teraz do polskiej wizji kwestii etycznych związanych ze sztuczną inteligencją.

Wojciech ORLIŃSKI

Konferencja jest bardzo interesująca. Pokazuje pewien konsensus, co konieczności regulacji. Do niedawna wizja ta nie była szeroko podzielana przez polską opinię publiczną. I wydaje mi się, że kolejne pokolenia uznają tę postawę ludności za ogromny błąd.

Pokazuje to różnice między przepisami poszczególnych krajów. Jest to nawet argument dla niektórych państw trzecich podkreślających słabość Europy w tej kwestii.

Moim zdaniem, musimy posuwać się do przodu w trzech kierunkach. Po pierwsze, musimy być w stanie ustalić, czy rozmawiamy z człowiekiem, czy z robotem. W drugim przypadku pamiętajmy, że nie zawsze mamy do czynienia z działaniami złośliwymi. Następnie, korzystanie ze sztucznej inteligencji nie może zwalniać użytkownika z jego odpowiedzialności. Wreszcie, przejrzystość musi stanowić regułę, jeśli chodzi o algorytmy.

Ponadto musimy zawsze być w stanie stosować środki odwoławcze. To właśnie odróżnia system demokratyczny od totalitarnego. W chwili obecnej mamy wrażenie, że w świecie Internetu nie ma możliwości stosowania środków odwoławczych. To musi się zmienić.

IV) Kwestia przejrzystości algorytmów stosowanych przez przemysłowców

Bernard BENHAMOU

Kwestia przejrzystości była wielokrotnie podnoszona, zwłaszcza w stosunku do Facebooka. Wspomnę o konsekwencjach zmian w algorytmach Facebooka i ich wpływie na liczbę osób, które wymieniały się informacjami o „Żółtych Kamizelkach”. Czy w chwili obecnej powinniśmy narzucić przejrzystość dużych platform w odniesieniu do ich algorytmów? Panie Ministrze, jakie jest pańskie stanowisko w tej sprawie?

Gérard LONGUET

Szczerze mówiąc, nie jesteśmy wystarczająco dojrzali, aby móc określić punkt równowagi pomiędzy poszanowaniem własności intelektualnej a potrzebą ochrony danych. Jednak ewentualne naruszenia dotyczące algorytmów, zwłaszcza w sektorze ochrony zdrowia, stawia ten temat w centrum debat.

Potwierdzam, że sztuczna inteligencja to fantastyczny atut w dziedzinie opieki zdrowotnej, ponieważ umożliwia przesyłanie i przetwarzanie danych w zupełnie nowy sposób. Mogłoby to się jednak zakończyć stworzeniem systemu, który byłby sprzeczny z

interesem ogólnym i miałby negatywny wpływ zarówno na badania medyczne, jak i na dobrostan pacjentów.

W odniesieniu do epoki, gdy byłem Ministrem Poczty i Telekomunikacji, zilustruję to ryzyko poprzez porównanie: wspomniane przeze mnie nadużycia można by porównać do bezpłatnych usług pocztowych, ale w ramach których użytkownik pozwoliłby listonoszowi przeczytać listy. Biorąc pod uwagę ilość zebranych danych, stawka ekonomiczna jest tutaj ogromna.

W chwili obecnej nasza wiedza na te tematy jest niewystarczająca. Rozwój sytuacji gospodarczej ogranicza wybór wielu przedsiębiorstw do alternatywy: przystosuj się lub giń. W każdym razie debaty w Parlamencie Europejskim wydają mi się bardzo interesujące, ponieważ faworyzują pojęciu wolności w stosunku do pojęcia regulacji.

Bernard BENHAMOU

Czy zgodnie z niemiecką wizją powinniśmy narzucić platformom przejrzystość stosowanych algorytmów?

Till STEFFEN

Dotychczas Unia Europejska i wszystkie państwa członkowskie ograniczyły się do przyjmowania nieodpowiednich standardów. Facebook musi podlegać przepisom antymonopolowym, tak jak inne firmy. Musimy zatem poważnie rozważyć wdrożenie wspomnianych przez Pana kontroli. Ten obszar gospodarczy musi angażować nas w taki sam sposób, jak pozostałe.

Bernard BENHAMOU

Jak Polska ustosunkowuje się do tej kwestii?

Konstanty RADZIWIŁŁ

Wydaje mi się, że popełniliśmy błąd polegający na zaufaniu niewidzialnej ręce, która ureguluje ten rynek. Przekonanie to opierało się na zachętach pochodzących z niektórych innych branż.

Na przykład w sektorze opieki zdrowotnej systemy prognostyczne mogą poczynić ogromne szkody, jeśli będą stosowane przez ubezpieczycieli lub pracodawców.

W odniesieniu do Facebooka pamiętam, że przedstawicielka tej firmy była obecna na naszej konferencji w Berlinie. Kiedy zakwalifikowała działalność swojej firmy jako reklamę, zareagowała cała sala. A dziś ta sama firma ogłasza wprowadzenie kryptowaluty. Co możemy myśleć na temat prawdziwych zamiarów Facebooka? Czy jest to sposób na zebranie jeszcze większej ilości danych?

Chciałbym również przytoczyć inny przykład: robot domowy sprzedawany przez Lidla. Niektórzy użytkownicy odkryli w nim mikrofon. Przeprowadzone dochodzenie nie pozwoliło na wyjaśnienie jego obecności. Niektórzy zakładają, że była to konfiguracja dla przyszłej podłączonej wersji robota.

Te konkretne przypadki pokazują nam, że nasi przeciwnicy są liczni i że musimy im poświęcić pełną uwagę. Rynek nie będzie w stanie sam się regulować. Sprawa Chin przypomniała mi pewną anegdotę. W czasach polskiego reżimu totalitarnego pytaliśmy, na czym polega różnica między demokracją a demokracją socjalistyczną. Odpowiedź brzmiała, to taka sama różnica jak ta między krzesłem a krzesłem elektrycznym.

Ta sytuacja jest w rzeczywistości dramatyczna. Ponadto wielką nieobecną w naszych debatach jest Rosja. Czasami główne zagrożenie nie pochodzi od krajów, które produkują technologię, ale od tych, które ją niewłaściwie używają.

Bernard BENHAMOU

Przypadek robota domowego dotyczył również rynku francuskiego, ponieważ był on wprowadzany do obrotu we wszystkich krajach europejskich.

Leonie BEINING

Uważam, że konieczne jest doprecyzowanie kwestii przejrzystości. Nie posuwając się aż do znajomości kodu źródłowego, obywatel powinien być w stanie wiedzieć, że dana decyzja została podjęta za pomocą algorytmu. Podobnie ważne byłoby informowanie o kryteriach stosowanych w procesie decyzyjnym.

V) Słabości Europy w zakresie sztucznej inteligencji

Bernard BENHAMOU

Dużo mówiliśmy o sprawach dotyczących Chin i Stanów Zjednoczonych. Wróćmy do Europy, aby przyjrzeć się jej słabościom. Obserwujemy wyjazd wielu utalentowanych osób, do pracy w zagranicznych firmach. Jakie są środki, aby zaradzić tej niefortunnej sytuacji? Co może powiedzieć na temat tej sytuacji André Gattolin?

André GATTOLIN

Francuska szkoła matematyczna jest rzeczywiście uznawana w dziedzinie sztucznej inteligencji. Tariq Krim przygotował doskonałe sprawozdanie na ten temat. Wnioski, które wyciągnął, pozostają całkowicie aktualne. Pokazał, jak najlepsze francuskie mózgi trafiły do Kalifornii. Kilka lat temu jeden z poprzednich rządów pogłębił tę tendencję, ograniczając system pomocy do 2,5-krotności SMIC, co ograniczyło zdolność francuskich przedsiębiorstw do reagowania na tę tendencję.

Bernard BENHAMOU

Rodzi to pytania o działania, jakie należy podjąć w ramach przepisów antymonopolowych.

André GATTOLIN

Absolutnie. Chciałbym wspomnieć przypadek firmy Skype, która umiera, ponieważ firma, która ją kupiła, chce skupić się na swoim własnym systemie komunikacji wewnętrznej.

Musimy również przedstawić inne propozycje w dziedzinie innowacji. Z naszymi możliwościami, całe obszary pozostają niewykorzystane. Na przykład sektor rolny może prowadzić do rozwoju wielu „inteligentnych systemów rolniczych”. To samo dotyczy zarządzania zasobami rybnymi. Bądźmy kreatywni, nie pozostawajmy wewnątrz logiki odtwarzania tego, co już istnieje.

Kwestia opodatkowania zysków osiąganych przez przedsiębiorstwa cyfrowe znajduje się w centrum dyskusji toczących się na forum G20. Chociaż Amerykanie nie są wobec niego wrogo nastawieni, nadal żądają, aby miało to zastosowanie do wszystkich firm.

Bernard BENHAMOU

Jakie inne narzędzia pozwoliłyby nam rozwinąć się w tych obszarach? Co o tym sądzi, Leonie Beining?

Leonie BEINING

Pytanie to należy zadać z perspektywy polityki przemysłowej. Talent, materiał i dane to trzy składniki sztucznej inteligencji. Jako takie, zasługują na większe inwestycje. Musimy zatem zapewnić ściślejszą współpracę w Europie, aby mogły powstać nowe pomysły.

Sprzeciwiam się czysto pesymistycznemu podejściu do sytuacji, które koncentruje się wyłącznie na zacofaniu Europy. Musimy wypracować inną wizję, trzecią drogę. Ponadto powinniśmy być dumni z dokonanych osiągnięć, ponieważ RODO to prawdziwy sukces.

Z pewnością działamy powoli, ale ta powolność stanowi cenę prawdziwej refleksji. Pytania muszą również wybiegać w przyszłość. Badania pokazują katastrofalny bilans sztucznej inteligencji w zakresie jej śladu ekologicznego. Musimy jeszcze bardziej skupić się na tych aspektach.

Bernard BENHAMOU

Jak Polska ocenia zdolność Europy do poprawy sytuacji?

Wojciech ORLIŃSKI

Jako dziennikarz, mogę wypowiadać się swobodnie. Jestem obywatelem polskim i jako taki, te debaty mnie zaskakują. Kiedy Polska przystąpiła do Unii Europejskiej, mieliśmy wrażenie, że państwa członkowskie z Zachodu posiadały wszystkie odpowiedzi na wszystkie pytania. Teraz, gdy sami jesteśmy konsultowani w tych sprawach, odnosimy dziwne wrażenie.

Z pewnością Europa potrzebowała czasu, aby rozwiązać niektóre problemy: potrzeba było siedmiu lat zarówno na ukończenie RODO, jak i na zakończenie procesu przeciwko Google. Wszystko zakończyło się sukcesem. Chociaż procedury w Stanach Zjednoczonych wydają się być szybsze, należy zauważyć, że nie istnieje tam ani RODO, ani wyrok skazujący Google. Dlatego też wydaje mi się, że trzecia droga, jaką obrała Europa, jest dość skuteczna.

Komentarze Tilla Steffena są bardzo istotne. Rzeczywiście, musimy ustanowić europejskiego lidera w tych dziedzinach, takiego jak Airbus we swojej branży.

Czym jest sztuczna inteligencja w praktyce? To umiejętności informatyczne i wolumeny danych. GAFA jest właścicielem obu. Żadna inna firma nie może się aktualnie z nią mierzyć. Nie brakuje perspektyw rozwoju i Europa musi odegrać w nim pełną rolę.

Bernard BENHAMOU

Jesteśmy świadomi, że opanowanie kwestii środowiska naturalnego może być częścią tego procesu.

Anthony COLOMBANI

Stan umysłu, który wyłania się z naszych debat, jest pozytywny, ponieważ pokazuje rzeczywistą gotowość do dalszych działań. Chciałbym podkreślić, że sztuczna inteligencja nie ogranicza się do Stanów Zjednoczonych i Chin. Wiele przykładów znajduje się w Europie.

Bernard BENHAMOU

Jednakże część konsumencka znajduje się głównie w Stanach Zjednoczonych.

Anthony COLOMBANI

Tak, ale nasza wizja tematu musi być globalna. Moim zdaniem musimy rozważyć pewną ulgę regulacyjną i lepiej przewidywać wpływ sztucznej inteligencji.

VI) Wdrażenie polityki rozwoju talentów

Bernard BENHAMOU

Jesteśmy świadkami zjawiska utraty talentów. Europa stała się centrum handlowym dla rekrutacji naszych najzdolniejszych umysłów. Czasami płace są pięciokrotnie wyższe, nawet dziesięciokrotnie, nie wspominając nawet o przypadku naukowców z CNRS. Jak możemy ograniczyć to zjawisko? Jakie byłyby sposoby odwrócenia tego trendu, André Gattolin?

André GATTOLIN

Stanowi to rzeczywiście problem. Z historycznego punktu widzenia, nasza liberalna wizja uniemożliwiła nam pomoc naszym przedsiębiorcom. Wtedy wdrożyliśmy różne systemy poziome, takie jak ulgi podatkowe. Wydaje mi się, że konieczny jest system pionowy. Przykład Google mówi sam za siebie: ta firma była w stanie zacząć niezwykle szybko rozwijać się, gdy nastąpiła integracja z administracją branży Obrony. Ponadto Unia Europejska musi wprowadzić politykę przemysłową.

Wymagałoby to utworzenia Europejskiej Rady ds. Innowacji. Nasz obecny model musi zatem zostać radykalnie zmodyfikowany, aby odwrócić ten trend.

Pytania od słuchaczy

Bernard BENHAMOU

Teraz odpowiemy na pytania z sali.

Z sali

Chciałbym dowiedzieć się więcej na temat pojęcia „blockchain”.

Te debaty są bardzo interesujące i cieszę się z ich wysłuchania. Jednakże rozwój sztucznej inteligencji wydaje się pomijać terytoria trudniej dostępne geograficznie, takie jak Antyle Francuskie.

Wojciech ORLIŃSKI

Ten temat jest bardzo złożony, często omawiam go z uczniami. Łańcuchy bloków mogą być dźwigniami rozwojowymi dla rozpoczęcia działalności gospodarczej. Są one różnie traktowane w różnych państwach. W tej sprawie Europa musi zająć stanowisko.

Jeśli chodzi o departamenty i terytoria zamorskie, rozumiem to poczucie izolacji.

Bernard BENHAMOU

Chciałbym zwrócić uwagę, że wszystkie nasze debaty są filmowane. W związku z tym nasi zagraniczni przyjaciele mogą łatwo znaleźć film na stronie internetowej Senatu.

Anthony COLOMBANI

Osobiście chciałbym wspomnieć przypadek Korsyki, który jest bardzo podobny do przypadku Antyli Francuskich. Powinniśmy czerpać inspirację z niektórych krajów, które postawiły na bardzo wysoki poziom szkoleń w zakresie technologii cyfrowej, takich jak Włochy. Wielu włoskich studentów jest rekrutowanych przez GAFA po ukończeniu studiów.

Z sali

Jestem prawnikiem specjalizującym się w dziedzinie nowych technologii. Po wysłuchaniu pana, dostrzegam ogólne pragnienie stanowienia prawa we wszystkich tych kwestiach. Nasza firma zajmuje się projektami długoterminowymi, dla których znajomość

przyszłych zmian regulacyjnych będzie miała kluczowe znaczenie w celu jak najlepszego wsparcia naszych klientów. Czy mają Państwo jakieś dalsze szczegóły dotyczące programu reform?

Konstanty RADZIWIŁŁ

Nie mogę skomentować sytuacji we Francji. Na szczeblu wspólnotowym uważam, że jedynym obszarem w odniesieniu, do którego ustanowiliśmy prawo, jest odpowiedzialność za produkt. Będziemy rzeczywiście pracować nad innymi aspektami, ale niemożliwe jest ogłoszenie harmonogramu.

Zakończenie: jak wygląda odpowiedź Unii Europejskiej?

Jean BIZET
Senator departamentu Manche, przewodniczący senackiej Komisji Spraw Europejskich

Niestety przewodniczący Senatu, pan Gérard Larcher, nie mógł uczestniczyć w tej konferencji. Jednakże, poprosił mnie o przesłanie następującej wiadomości.

Szanowne Panie i Szanowni Panowie Przewodniczący,

Szanowni Państwo Parlamentarzyści,

Szanowni Państwo,

Bardzo cieszę się z organizacji naszej trzeciej konferencji w formacie „Trójkąta Weimarskiego" i dziękuję za obecność Państwa w Pałacu Luksemburskim.

Chciałbym podziękować w zwłaszcza naszym niemieckim i polskim gościom, a w szczególności panu Tillowi Steffenowi, przewodniczącemu Komisji Prawa Federalnego, oraz panu Łukaszowi Mikołajczykowi i panu Ministrowi Konstantemu Radziwiłłowi, członkom polskiego Senatu, a także moim kolegom senatorom za ich obecność i aktywny udział.

To właśnie w 2016 r. powzięliśmy wraz z marszałkiem Senatu RP, panem Stanisławem Karczewskim i ówczesnym prezydentem Bundesratu, panem Stanislasem Tillichem, pomysł zorganizowania serii trzech konferencji parlamentarnych w formacie „Trójkąta Weimarskiego".

Pierwsza konferencja, która odbyła się w Warszawie 4 grudnia 2017 r., poświęcona była walce z mową nienawiści w Internecie.

Druga konferencja odbyła się w Berlinie 22 października 2018 r. i dotyczyła walki z fałszywymi wiadomościami.

Nasza trzecia konferencja odbywająca się w Paryżu, jest zatem ostatnią z tego cyklu i pozwala nam na stworzenie podsumowani i przygotowanie perspektyw na przyszłość.

Zdecydowaliśmy się zatytułować to trzecie wydanie „Bezpieczeństwo cybernetyczne, ochrona danych i sztuczna inteligencja: jakie wyzwania dla Europy?"

Uważamy, że tylko ogólnoeuropejska reakcja będzie mogła stawić czoła wyzwaniom związanym z bezpieczeństwem cybernetycznym i sztuczną inteligencją.

W tym kontekście jesteśmy przekonani, że Francja, Niemcy i Polska mogą odegrać użyteczną rolę jako bodziec dla naszych europejskich partnerów oraz instytucji europejskich.

W obliczu wzrostu liczby ataków cybernetycznych, w celach przestępczych, szpiegowskich lub sabotażowych, bezpieczeństwo cybernetyczne to jeden z głównych problemów bezpieczeństwa narodowego.

Od czasu sprawozdań Romani i Bockel Senat odgrywa pionierską rolę w tej dziedzinie, wzywając do uświadomienia w kwestiach związanych z bezpieczeństwem cybernetycznym i do wzmacniania środków do walki z tym zagrożeniem.

Komisja Senacka do Spraw Zagranicznych, Obrony i Sił Zbrojnych wzmocniła, podczas analizy ostatniej ustawy o programowaniu wojskowym, środki, którym dysponuje ANSSI.

Senat to również czujny strażnik ochrony danych, zarówno na szczeblu krajowym, jak i europejskim, dzięki Komisji Prawnej i Komisji Spraw Europejskich.

Wraz z pojawieniem się połączonych przedmiotów ochrona danych stanie się niewątpliwie kwestią zasadniczą dla zachowania równowagi między bezpieczeństwem a swobodami jednostki.

Wzrost liczby wypowiedzi na tle nienawiści, antysemityzmu, rasizmu, dezinformacji i manipulacji w Internecie i sieciach społecznych stanowi również wyzwanie dla naszych demokracji.

Od czasu spraw Snowdena i Cambridge Analytica jesteśmy świadomi niebezpieczeństwa manipulacji i dezinformacji dla funkcjonowania naszych demokracji.

Senat bardzo dużo pracował nad kwestią dostosowania naszego prawa do technologii cyfrowej, szczególnie w Komisji Prawa i Komisji Kultury, Edukacji i Komunikacji, aby osiągnąć lepszą równowagę między wolnością wypowiedzi w Internecie a walką z nienawiścią.

Zgromadzenie Narodowe i Senat zostaną wkrótce poproszone o wydanie opinii w sprawie projektu ustawy zainspirowanej niemieckim ustawodawstwem mającym na celu wzmocnienie obowiązku operatorów platform do usuwania nielegalnych treści w ciągu 24 godzin lub nałożenia na nich surowych kar finansowych.

Sztuczna inteligencja podnosi istotne kwestie demokratyczne, prawne, etyczne i przemysłowe, w szczególności w odniesieniu do przejrzystości algorytmów. Za pośrednictwem Parlamentarnego Biura Oceny Wyborów Naukowo-Technicznych Senat chciał ściśle monitorować te kwestie i wnieść wkład w dyskusje na temat dostosowania naszych ram prawnych.

Niezależnie od tego, czy jest to bezpieczeństwo cybernetyczne, czy też sztuczna inteligencja, tylko ogólnoeuropejska reakcja byłaby w stanie odpowiedzieć wyzwaniom, o czym świadczą prace przeprowadzone przez Komisję Spraw Europejskich Senatu.

W kwietniu ubiegłego roku na wniosek grupy republikanów, Senat powołał komisję śledczą ds. suwerenności cyfrowej. Komisja rozpoczęła przesłuchania i oczekuje się, że przedstawi swoje wnioski we wrześniu. W obliczu amerykańskich lub chińskich gigantów, celem jest zapobieżenie temu, by Unia Europejska stała się „kolonią cyfrowego świata", jeśli użyć tytułu sprawozdania informacyjnego Senatu.

We wszystkich tych dziedzinach niezwykle przydatne jest podejście porównawcze między Francją, Niemcami i Polską. Myślę tu w szczególności o wyzwaniach w zakresie bezpieczeństwa, które wynikają z rozmieszczenia 5G, oraz o potrzebie koordynacji na szczeblu europejskim.

Nasze trzy kraje mogą również odegrać pożyteczną rolę w Unii Europejskiej, zapewniając wspólne reakcje na te wyzwania. Jestem przekonany, że parlamenty krajowe, a w szczególności wyższe izby, mogą się do tego przyczynić.

Z okazji 20. sesji Zgromadzenia Senatów Europejskich, która odbyła się w Paryżu w dniach 13-15 czerwca, podpisaliśmy wspólną deklarację z prezydentem Bundesratu Danielem Guntherem i marszałkiem Senatu RP Stanisławem Karczewskim. W tej deklaracji zgodziliśmy się w szczególności:

- *Kontynuować wymianę doświadczeń i dobrych praktyk,*
- *Kontynuować dialog między parlamentarzystami, ekspertami, specjalistami i przedstawicielami społeczeństwa obywatelskiego,*
- *Zbadać środki legislacyjne mające na celu zwiększenie świadomości społecznej w zakresie zagrożeń cybernetycznych, zwłaszcza wśród najmłodszych członków społeczeństwa.*

Tak więc dzisiaj położyliśmy trzeci kamień, ale nasz budynek jest jeszcze daleki od ukończenia. W ramach Weimaru będziemy musieli kontynuować naszą pracę w przyszłości,. Dziękuję za uwagę.

Dziękuję Państwu za obecność i uwagę, a także za jakość debat.