Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

Poniedziałek 25 listopada 2019 r. w godz. 19.00–22.30
w Parlamencie Europejskim
STRASBURG

Wysłuchanie kandydata Yanna PADOVY

1. Czy może Pan podać powody, dla których ubiega się Pan o to stanowisko, i dlaczego uważa się Pan za odpowiedniego kandydata?

Moja dotychczasowa kariera zawodowa umożliwiła mi **wszechstronne spojrzenie na ochronę danych**, z którą to dziedziną mam do czynienia zawodowo **od 20 lat**. Na początku poznałem ją od strony ustawodawcy – w Zgromadzeniu Narodowym – pracując nad transpozycją dyrektywy 95/46 oraz nad różnymi innymi projektami ustaw, w tym nad ustawą o utworzeniu rejestru służącego nadzorowi nad przestępcami seksualnymi. W Zgromadzeniu Narodowym, gdzie **jako administrator** podlegałem obowiązkowi **ścisłej neutralności**, nauczyłem się współpracować z pochodzącymi z wyboru osobami **o różnych przekonaniach politycznych** i negocjować kompromisowe rozwiązania dotyczące tekstów ustawodawczych. Później podobne zadania realizowałem w Komisji Europejskiej, gdzie pracowałem nad pierwszymi wersjami RODO. To **doświadczenie w charakterze doradcy ustawodawców** wydaje mi się szczególnie istotne dla Europejskiego Inspektora Ochrony Danych (EIOD) w jego roli względem Parlamentu i Rady.

Jako sekretarz generalny francuskiego urzędu ochrony danych (CNIL) stworzyłem w ramach transpozycji tego rozporządzenia „nowy CNIL”, wyposażony w szerokie i różnorodne uprawnienia. **Zmieniono procedury i organizacja CNIL, zagwarantowano wykonalność środków przymusu i uprawnień kontrolnych, wprowadzono nowe usługi i narzędzia dla użytkowników** itd. Aby wyjaśnić, na czym polegają te nowe uprawnienia, zainicjowałem ambitną politykę komunikacyjną, w tym na szczeblu europejskim. Z uwagi na nowo przydzielone EIOD zadania to **doświadczenie we wprowadzaniu zmian**, w **zarządzaniu**, we wdrażaniu nowych uprawnień, **w rygorystycznym zarządzaniu budżetem**, we wdrażaniu narzędzi i prowadzeniu zręcznej **polityki komunikacyjnej** wydaje mi się kluczowe dla pełnienia funkcji EIOD.

Jako członek Komisji Regulacji Energetyki (CRE) nadzorowałem sporządzanie sprawozdania z zarządzania danymi przez operatorów sieci energetycznych. Zadania tych operatorów sieci szybko ewoluują wraz z wprowadzaniem „inteligentnych sieci” i związanym z nimi masowym gromadzeniem danych. Pojawiają się zatem nowe możliwości, ale i nieznane dotąd zagrożenia, takie jak cyberprzestępczość. Jako EIOD będę korzystać także i z tego doświadczenia w

zakresie tworzenia nowych ram regulacyjnych w **strategicznym sektorze przemysłowym**, **w służbie końcowym konsumentom** i w trosce o **zaufanie do usług cyfrowych**.

Jako doradca strategiczny w Biurze Komisarza ds. Informacji (Information Commissioner's Office (ICO) – Zjednoczone Królestwo) **pracuję obecnie nad powiązaniem między regulacją a innowacją**. Od 2016 r. moja rola polegała na opracowaniu projektu **środowiska testowego** i na towarzyszeniu ICO w tym procesie aż do jego materialnej realizacji. Na szczeblu europejskim, w szczególności **w Parlamencie**, potrzebna będzie debata na temat innowacji w służbie dobra publicznego, zwłaszcza w świetle europejskich ambicji w dziedzinie sztucznej inteligencji. Refleksja prowadzona przeze mnie na ten temat, jak również moja działalność dydaktyczna i moje publikacje naukowe będą mi bardzo przydatne w roli doradcy Parlamentu.

Ponadto wykonuję zawód adwokata w międzynarodowej kancelarii. Doradzam przedsiębiorstwom w zakresie danych osobowych przy opracowywaniu innowacyjnych projektów i w zarządzaniu nimi. Problematyka ochrony danych staje się jednym z czynników wpływających na konkurencyjność i wyróżnianie się przedsiębiorstw. Jest to również wyższy współczynnik ryzyka ze względu na wysokość kar przewidzianych w RODO. Moja rola doradcza ma zatem, tym bardziej dziś, charakter strategiczny i wieloaspektowy. **Poznanie i zrozumienie wyzwań i sposobu funkcjonowania przedsiębiorstw od wewnątrz**, ograniczeń i celów związanych z ich transformacją cyfrową to moim zdaniem **konieczny warunek odpowiedniej realizacji** zadań przypisanych EIOD.

Moja zróżnicowana kariera zawodowa stanowi gwarancję wielodyscyplinarnej wiedzy fachowej, strategicznej wizji wyzwań, otwartości na środowisko międzynarodowe, ale również i pragmatyzmu. Moja ścieżka zawodowa ukazuje **moją zdolność do budowania pomostów**: **między różnymi dyscyplinami** prawnymi, **między prawem a technologiami**, między **prawem a gospodarką**, między **systemami prawnymi różnych państw**, między **instytucjami a innymi podmiotami, w tym politycznymi, o czasem rozbieżnych interesach** oraz między **różnymi kulturami**. Moja kariera odzwierciedla również moje **przywiązanie do europejskiej koncepcji ochrony danych**, moją zdolność do jej obrony i **propagowania jej** na szczeblu międzynarodowym. To przywiązanie wynika również z **mojego pochodzenia**, gdyż jestem w połowie Szwedem po matce, moi przodkowie ze strony ojca pochodzą z Polski wschodniej, a jednocześnie noszę nazwisko będące nazwą włoskiego miasta, w którym ci przodkowie znaleźli schronienie.

Na koniec pragnę dodać, że **w mojej karierze zawodowej kieruję się zasadą niezależności**. Było tak, gdy postanowiłem pracować dla CNIL i CRE, które są niezależnymi urzędami. Jest tak również i dziś, gdyż w zawodzie adwokata jest ona wymogiem etyki zawodowej. Niezależność ta nie jest tylko deklarowana, lecz przejawia się w czynach: świadczą o niej **moje artykuły** naukowe dotyczące prawa do bycia zapomnianym idące w tym samym kierunku co decyzja TSUE (C-507/17) lub moja niedawna **mowa obrończa przed TSUE** w sprawie kontroli państwa (C-511/18). Niezależność jest wymagającą dyscypliną. Musi obejmować **dialog ze wszystkimi zainteresowanymi stronami**, w przeciwnym razie przekształca się w odizolowaną samowystarczalność. Takiej właśnie wizji niezależności będzie potrzebować EIOD – wymagającej, lecz **konstruktywnej, otwartej, lecz stanowczej** i w taki sposób chcę być niezależny **w służbie Parlamentowi**.

2. Czy mógłby Pan opisać swoją wizję przyszłości organu, którym kierowałby Pan jako EIOD, w tym ewentualne wyzwania, jakie Pan przewiduje, oraz Pańskie priorytety dla tego niezależnego organu?

Wraz z szybkim rozwojem **sztucznej inteligencji**, uczeniem się maszyn i internetem rzeczy Europa stoi w obliczu **bezprecedensowych wyzwań etycznych**. Biorąc pod uwagę, że ilość tworzonych danych podwaja się co 24 miesiące, jak regulować algorytmy, które samoistnie się zmieniają i wydają się czasem wymykać spod kontroli swoim twórcom? Jak zapewnić przejrzystość i zrozumiałość tych narzędzi, które opanowują naszą codzienność? Jak zagwarantować ich obiektywność i oceniać ich stronniczość? W jaki sposób je skorygować w razie dyskryminującego podejścia? Wyzwania te są tym bardziej istotne, że **Europa jest rozdarta między dwoma modelami regulacyjnymi**: modelem stosowanym w Stanach Zjednoczonych, gdzie brak jest horyzontalnych przepisów federalnych dotyczących danych i to sędzia czy nawet sektorowy organ regulacyjny orzeka w tej sprawie *a posteriori*, a modelem chińskim, który charakteryzuje się państwową hipercentralizacją dostępu do danych.

W ramach tej **geopolityki danych** w tym zaledwie wykluwającym się świecie cyfrowym Europa musi objawić się jako nowy ważny gracz. Komisja ogłosiła, że zamierza w ciągu 100 dni przedstawić wniosek w sprawie sztucznej inteligencji. Europa **dysponuje środkami na miarę swoich ambicji**, ponieważ posiada już solidne ramy prawne, które mogą posłużyć za **fundament** tego nowego rozporządzenia – **RODO**. W akcie tym przewidziano odpowiednie zasady, takie jak rozliczalność, przejrzystość, prawo jednostek do decyzji podjętej nie tylko na podstawie automatycznego przetwarzania. Opierając się na RODO, Europa może i musi **doprowadzić do etycznego stosowania sztucznej inteligencji – odpowiedzialnej, korzystnej dla ludzi i społeczeństwa jako całości**. W ramach **tworzenia** tego **europejskiego i humanistycznego podejścia do sztucznej inteligencji** EIOD ma do odegrania istotną rolę jako doradca podsuwający pragmatyczne i innowacyjne propozycje **Parlamentowi, który jest instytucją najbardziej nadającą się** do tego, by **demokratycznie** stworzyć to europejskie podejście. Co do istoty, można by rozważyć wprowadzenie: – podejścia ukierunkowanego na zagrożenia, które mogłoby się oprzeć na prawie do eksperymentowania, – ulepszonych mechanizmów certyfikacji, – wzmocnionej korekty i przejrzystości, a nawet identyfikowalności danych i stosowanych algorytmów (być może idącej w kierunku „paszportu" danych). Jest to pierwsze poważne wyzwanie, które trzeba będzie podjąć również **na szczeblu międzynarodowym**. **EIOD** będzie musiał być **orędownikiem tego europejskiego podejścia**.

Drugie wyzwanie strategiczne dla EIOD wynika z **rosnącej wartości danych oraz ze złożoności gospodarki opartej na danych i jej zdolności do ciągłego doskonalenia się**. Rozumienie łańcucha wartości oraz **identyfikowanie pojawiających się tendencji** i nowych podmiotów stają się warunkiem wstępnym świadczenia odpowiedniego doradztwa – **elastycznego** i już nie tylko reaktywnego, a **proaktywnego**. Dlatego EIOD **będzie musiał wzmocnić** funkcjonujące mechanizmy **współpracy** z organami europejskimi odpowiedzialnymi za **konkurencję** i z **krajowymi organami ochrony danych**, a także rozwijać partnerstwa z ośrodkami prowadzącymi badania w dziedzinie **gospodarki**, **cyberbezpieczeństwa** i **socjologii** zastosowań technologii. Przede wszystkim jednak będzie musiał zwiększyć swoją zdolność do **prospektywnej analizy technologii** i do interwencji, **dywersyfikując profile pracowników z korzyścią dla swej niezależności**.

Mam **doświadczenie w rozwijaniu takiej zdolności do prospektywnej analizy technologii**, gdyż w CNIL stworzyłem **laboratorium eksperckie**, jedno z pierwszych w Europie, jednocześnie zwiększając odsetek inżynierów wśród personelu z 3% do 10% w ciągu 6 lat. Ochrona danych nie może już funkcjonować w **izolacji**. Aby służyć **odpowiednim, proaktywnym i wielodyscyplinarnym doradztwem Parlamentowi, Radzie i Komisji, EIOD musi się** bardziej otworzyć i **skupić** na **nowym projekcie strategicznym**. Zobowiązuję się **opracować go na zasadzie współpracy** w ciągu 6 miesięcy od objęcia stanowiska w konsultacji z **zainteresowanymi podmiotami**, ponieważ **niezależność nie** jest **tożsama z samowystarczalnością**.

Trzecie wyzwanie dotyczy wymiany i przekazywania danych między państwami, w tym państwami trzecimi, na potrzeby walki z przestępczością. **TSUE i Parlament zajęły zdecydowane stanowiska**, na których EIOD będzie mógł opierać się przy wykonywaniu swoich zadań zarówno doradczych, jak i kontrolnych (zob. pytanie 3).

Ostatnie wyzwanie stojące przed EIOD wynika z jego **roli nadzorczej** w stosunku do instytucji europejskich. EIOD musi być inspektorem **przewidywalnym, uczciwym i wiarygodnym**. W tym celu musi nadal pomagać instytucjom europejskim w działaniu zgodnym z przepisami, **wspierać ich dojrzewanie**, na przykład oferując im **nowe narzędzia** na potrzeby rozliczalności, takie jak wzory umów o podwykonawstwo czy też narzędzia samooceny, tematyczne **przewodniki praktyczne**, pogłębione szkolenia z zakresu cyberbezpieczeństwa. EIOD będzie też musiał zwiększyć swoje kompetencje w zakresie **własnej zdolności do prowadzenia kontroli** na miejscu i na podstawie dokumentów, co wymaga **szczególnych kompetencji**. Wiem o tym, gdyż **utworzyłem służbę kontrolną w CNIL**. Ponadto EIOD będzie musiał **opublikować roczny program kontroli i złożyć sprawozdanie z jego realizacji**, w szczególności **przed Parlamentem**. To ważne również dla jego **wiarygodności**, zarówno w UE, jak i poza jej granicami.

Z uwagi na te wyzwania **EIOD będzie potrzebować pełnego wsparcia Parlamentu**, aby uzyskać zwiększenie zasobów, które pozostają niedostateczne w świetle stojących przed nim zadań i wzywań.

3. W jaki sposób zamierza Pan wypełnić rolę przyznaną EIOD z mocy prawa i dotyczącą nadzoru nad agencjami w obszarze wymiaru sprawiedliwości i spraw wewnętrznych, a także jakie jest Pana zdanie na temat wymiany danych osobowych przez agencje WSiSW oraz z tymi agencjami, w szczególności w odniesieniu do nadzoru nad przekazywaniem danych osobowych do państw trzecich?

Aby skutecznie kontrolować przetwarzanie danych europejskich agencji sądowych i policyjnych, warto **znać przebieg procedur karnych**, instytucji sądowych i służb zajmujących się zwalczaniem przestępczości. Pod tym względem szczególnie istotne wydaje mi się moje doświadczenie w Komisji Prawnej Zgromadzenia Narodowego i w CNIL (francuski urząd ochrony danych).

W Komisji Prawnej zajmowałem się prawem karnym, monitorowaniem budżetu administracji więziennej oraz prawem w zakresie danych osobowych. W tym kontekście przez 7 lat pracowałem nad wszystkimi tekstami prawa karnego, a w szczególności nad bazą danych i narzędziami nadzoru nad sprawcami ciężkich przestępstw seksualnych (baza „FIJAIS”).

Co do CNIL – przez długi czas był to jeden z niewielu organów ochrony danych w Europie o kompetencjach w zakresie uprzedniej i następczej kontroli baz policyjnych i sądowych. Dlatego jako sekretarz generalny w latach 2008 i 2009 zorganizowałem **pierwszą ogólną kontrolę bazy danych policji sądowej** (bazy STIC) pod nadzorem właściwych prokuratorów Republiki. Za czasów tej kontroli baza STIC zawierała dane dotyczące 36 mln osób. Kontrola trwała ponad rok, w jej ramach przeprowadzono 19 inspekcji na miejscu, a do 34 sądów reprezentujących 50 % działalności w zakresie prawa karnego we Francji wysłano kwestionariusze oraz pytania techniczne dotyczące środków bezpieczeństwa i możliwości śledzenia powiązań między danymi. Ponadto prawo dostępu osób do danych przetwarzanych przez policję wykonywano wówczas wyłącznie w sposób zwany „pośrednim", a mianowicie CNIL wykonywała to prawo w imieniu osoby, która o to wystąpiła, co zresztą EIOD może robić na podstawie art. 84 rozporządzenia 2018/1725. To **wyjątkowe doświadczenie w zakresie kontroli i stosowania prawa do dostępu pośredniego** (prawie 4000 wniosków rocznie składanych do CNIL) będzie dla mnie szczególnie przydatne na stanowisku EIOD.

EIOD działa bowiem w **złożonych ramach prawnych**, które będą ewoluować w trakcie kolejnej kadencji. Pomimo przyjęcia rozporządzenia 2018/1725 i przepisów jego rozdziału IX uprawnienia EIOD nadal różnią się w poszczególnych przypadkach, ponieważ opierają się na kilku szczegółowych aktach prawnych. Dotyczy to przetwarzania danych operacyjnych przez Europol, Eurojust czy Prokuraturę Europejską. Uprawnienia EIOD różnią się tutaj, ponieważ nie może on nałożyć grzywny administracyjnej, wydać nakazu zawieszenia międzynarodowego przepływu danych ani też skierować upomnienia do Prokuratury Europejskiej. Nie może też orzec zakazu przetwarzania danych wobec Eurojustu i Prokuratury Europejskiej, inaczej niż w przypadku Europolu.

Obecnie obowiązujące systemy prawne pozwalają jednak **EIOD na sprawowanie rygorystycznej kontroli nad tymi agencjami – kontroli absolutnie niezbędnej ze względu na nieuniknione ryzyko związane z przetwarzaniem** takich danych, **a także z uwagi na perspektywę interoperacyjności** niektórych systemów informacyjnych. To właśnie w przypadku przekazywania danych ryzyko jest największe, a kontrole należy prowadzić z najwyższą dokładnością. W razie gdy Komisja nie wyda decyzji stwierdzającej odpowiedni stopień ochrony na podstawie dyrektywy 2016/680, rola EIOD będzie kluczowa.

Taka kontrola funkcjonuje już w odniesieniu do zawartych między Unią a państwami trzecimi umów dotyczących przekazywania danych przez Europol. Trzeba ją kontynuować na stale podtrzymywanym poziomie rygorystyczności. Jeśli chodzi o Eurojust i Prokuraturę Europejską, inspektor będzie musiał korzystać z powierzonych mu uprawnień kontrolnych, aby dokładnie upewniać się, że **przekazywanie danych odbywa się w myśl przepisów określonych w odpowiednich rozporządzeniach i zgodnie z wymogami TSUE**. Istnieje realne ryzyko, że w państwach trzecich przekazane dane będą wykorzystywane do innych celów, trzeba zatem prowadzić ścisłą kontrolę w tym zakresie.

Aby **zapobiec fragmentaryzacji** systemów kontroli, a tym samym osłabieniu poziomu ochrony danych osobowych w tej niezwykle sensytywnej dziedzinie, w art. 98 rozporządzenia 2018/1725 wprowadzono „klauzulę rendez-vous" (przewidującą termin 30 kwietnia 2022 r.). W klauzuli tej zwrócono się do Komisji o dokonanie przeglądu aktów szczegółowych, aby ocenić ich zgodność z dyrektywą 2016/680 i wskazać ewentualne rozbieżności, które mogą spowodować taką fragmentaryzację. Rola EIOD będzie decydująca, jeśli chodzi o dzielenie się doświadczeniem oraz doradzanie Komisji, Radzie i Parlamentowi.

W związku z powyższym wydaje mi się **niezbędne, aby EIOD**: i) opracował na początku 2020 r. **wieloletni program kontroli** uwzględniany w programie rocznym (zob. odpowiedź na pytanie 2); ii) zwiększył swoje **kompetencje** i dostępne środki z myślą o zadaniach w zakresie kontroli na miejscu; iii) rozwijał pogłębioną **koordynację** z **krajowymi organami ochrony danych** z uwagi na „mieszany” charakter danych przetwarzanych przez te agencje; iv) wyraźniej i szczegółowiej **zdawał sprawę** z realizacji swoich obowiązków nadzorczych; v) stworzył **narzędzia służące wspomaganiu** i zapewnianiu zgodności z przepisami na potrzeby współpracy z zespołami wspomnianych agencji.