



Wyzwania dla Parlamentu Europejskiego nowej kadencji

Poprzednia kadencja Parlamentu Europejskiego obfitowała w debaty i decyzje istotne z perspektywy praw i wolności obywatelskich. Obok wielu pozytywnych zmian, przyjęto również propozycje, które – zdaniem organizacji społecznych – podważają europejskie standardy ochrony praw człowieka. Rozpoczęta właśnie kadencja Parlamentu daje szansę na skorygowanie tego kierunku w niektórych kwestiach. Poniżej prezentujemy siedem procesów politycznych, na które posłowie do Parlamentu Europejskiego powinni w najbliższej przyszłości zwrócić szczególną uwagę.

1) Reforma ochrony danych osobowych

Reforma ochrony danych została zapoczątkowana przez Komisję Europejską w 2012 r. Jest to kluczowy proces polityczny, który przesądzi o europejskim standardzie ochrony prawa do prywatności na kolejne kilkadziesiąt lat. Niezwykle intensywne prace w Parlamencie Europejskim – w ich trakcie złożono m.in. 4 tys. poprawek – zakończyły się przyjęciem przez europosłów dwóch projektów (rozporządzenia i dyrektywy), które składają się na pakiet reformatorski. Obecnie oba projekty są procedowane na forum Rady Unii Europejskiej. Po wypracowaniu wspólnego stanowiska przez rządy państw członkowskich, rozpocznie się ostatnia – kluczowa – faza tzw. trilogu, czyli negocjacji między Radą UE, Parlamentem i Komisją Europejską.

Nasze postulaty:

- Pomimo, że Parlament Europejski przyjął już oficjalnie stanowiska w sprawie reformy ochrony danych osobowych, na dalszym etapie prac eurodeputowani nadal mają ważną rolę do odegrania. W szczególności, eurodeputowani mogą aktywnie śledzić proces negocjacji (trilogu) oraz pełnić funkcję kontrolną wobec działań podejmowanych przez wyznaczonego posła-sprawozdawcę.
- Eurodeputowani (szczególnie zasiadający w komisjach LIBE i JURI) powinni stać na straży jakości rozwiązań, jakie pojawią się w ostatecznie wynegocjowanym tekście dyrektywy i rozporządzenia o ochronie danych osobowych, dbając o zapewnienie odpowiedniego poziomu ochrony praw obywateli.
- Dodatkowo, Parlament Europejski powinien naciskać na rządy krajowe oraz władze Unii Europejskiej by prace nad reformą były prowadzone sprawnie, zapewniając szybkie przyjęcie dobrych rozwiązań prawnych.

Szczegółowe postulaty Fundacji Panoptykon dotyczące reformy ochrony danych są zawarte w załączonym opracowaniu : „Reforma europejskiego prawa o ochronie danych osobowych. Podsumowanie”¹

¹ Publikacja dostępna pod adresem

http://panoptykon.org/sites/panoptykon.org/files/panoptykon_ochrona_danych_brief_03.07.13.pdf.

2) Amerykańskie programy masowej inwigilacji

W czerwcu 2013 r. Edward Snowden ujawnił informacje o skali amerykańskich programów masowej inwigilacji. Sprawa PRISM wywołała gorące dyskusje w różnych gremiach politycznych. Parlament Europejski prowadził w tej sprawie niezależne śledztwo. Raport końcowy potwierdził istnienie programów masowej inwigilacji i wskazał, że naruszają one prawa człowieka. Europosłowie w rekomendacjach końcowych opowiedzieli się za wzmocnieniem mechanizmów kontroli nad służbami specjalnymi oraz zobowiązali Komisję Europejską do zawieszenia porozumień, które w praktyce nie gwarantują odpowiednich standardów ochrony prywatności (chodzi o program Safe Harbour i umowę w sprawie przekazywania danych z systemu SWIFT, przynajmniej do czasu wyjaśnienia wątpliwości dotyczących dostępu Amerykanów do danych bankowych). Parlament zagroził też odmową zgody na przyjęcie Transatlantyckiego Partnerstwa na rzecz Handlu i Inwestycji (TTIP), jeśli Amerykanie nie zaprzestaną masowej inwigilacji na terytorium UE. Swój sprzeciw wobec technologii masowego przetwarzania danych dla celów bezpieczeństwa wyraziło również Zgromadzenie Ogólne ONZ.

Nasze postulaty:

- Europosłowie powinni konsekwentnie domagać się, by władze krajowe i unijne dążyły do zablokowania programów masowej inwigilacji oraz wyjaśnienia roli państw europejskich w ich dotychczasowej realizacji.
- Parlament Europejski powinien aktywnie uczestniczyć w procesach politycznych dotyczących relacji z USA, szczególnie w zakresie przekazywania danych osobowych i walki z terroryzmem.
- W sytuacji dalszego naruszania przez USA europejskich standardów ochrony danych osobowych, Parlament Europejski powinien zrealizować zapowiedziane w poprzedniej kadencji sankcje: domagać się od Komisji Europejskiej zawieszenia porozumień, które pozwalają na swobodny przepływ danych, oraz odmówić zgody na przyjęcie TTIP.

3) Transfery danych do USA

Stany Zjednoczone w powszechnej opinii nie są bezpiecznym krajem z perspektywy ochrony danych osobowych. Od 2000 r. istnieje program Safe Harbour, który umożliwia transfer danych z podmiotów działających na terenie Unii Europejskiej do amerykańskich firm. Liczne opracowania i ewaluacje dowodzą, że program Safe Harbour nie zapewnia dostatecznej ochrony praw Europejczyków. Obecnie Komisja Europejska rozważa zawieszenie programu lub jego głęboką rewizję. Jednocześnie, od 2012 r. Komisja prowadzi z Waszyngtonem rozmowy w sprawie tzw. porozumienia parasolowego, które ma zapewnić obywatelom Unii Europejskiej dostateczny poziom ochrony prywatności w kontekście działań organów ścigania i wymiaru sprawiedliwości.

Nasze postulaty:

- Europosłowie powinni aktywnie śledzić proces podejmowania decyzji w sprawie dalszego obowiązywania programu Safe Harbour. Uważamy, że Parlament Europejski powinien wyrazić swoje zdanie w tej sprawie
- Z programem Safe Harbour oraz umową parasolową wiążą się liczne zagrożenia dla

obniżenia standardu ochrony danych osobowych Europejczyków. Eurodeputowani powinni więc zadbać by ten poziom ochrony nie uległ dalszej erozji w trakcie negocjacji ze stroną amerykańską. Przyjęte rozwiązania powinny w mocny sposób gwarantować silny poziom ochrony Europejczyków.

Szczegółowe uwagi Fundacji Panoptykon dotyczące programu Safe Harbour znajdują się w załączonym opracowaniu: „Safe Harbour – czyli jak (nie)bezpieczne są dane Europejczyków w Stanach Zjednoczonych”².

4) Dane pasażerów linii lotniczych

Na przestrzeni ostatnich lat Unia Europejska podpisała liczne umowy międzynarodowe – w tym z Kanadą, USA czy Australią – w sprawie przekazywania danych pasażerów linii lotniczych. Komisja Europejska zaproponowała również stworzenie europejskiego systemu danych PNR, który miałby służyć celom bezpieczeństwa. Z masowym i przewencyjnym wykorzystywaniem danych pasażerów linii lotniczych przez organy ścigania i służby specjalne wiąże się szereg problemów i zagrożeń w sferze ochrony praw człowieka (w szczególności naruszenie prawa do prywatności i zasady domniemania niewinności). Ostatnio udostępnienia danych PNR przez europejskie linie lotnicze w podobnych celach zażądała również Rosja. Istnieją podstawy aby sądzić, że podobne żądania mogą wysunąć w najbliższym czasie takie kraje jak Arabia Saudyjska, Kuba czy Korea Płd.

Nasze postulaty:

- Europosłowie powinni sprzeciwić się stworzeniu europejskiego systemu wykorzystywania danych PNR ze względu na związane z nim nieproporcjonalne naruszenie prawa do prywatności.
- Parlament Europejski nie może dopuścić do tego, by dane Europejczyków były przekazywane do krajów nie spełniających europejskich standardów praw człowieka.
- Eurodeputowani powinni brać aktywny udział w procesie negocjowania i przyjmowania umów o przekazywanie danych PNR do krajów trzecich. Umowy takie nie mogą prowadzić do wyłomu w ochronie praw podstawowych.

5) Transatlantyckie Partnerstwo na rzecz Handlu i Inwestycji

Od 2013 r. Unia Europejska prowadzi negocjacje z USA w sprawie Transatlantyckiego Partnerstwa na rzecz Handlu i Inwestycji (TTIP). Już teraz europejsko-amerykańskie rozmowy wywołują ogromne emocje. Istnieją obawy, że umowa może doprowadzić do nadmiernej deregulacji, ułatwić tworzenie monopolu i wprowadzanie rozwiązań sprzecznych ze standardami ochrony prawami człowieka, jak również forsowanie rozwiązań przyjaznych tylko dla dużych firm, a nie obywateli. Dlatego organizacje społeczne po obu stronach Atlantyku domagają się większej przejrzystości procesu negocjacji oraz wzmocnienia w nich roli Parlamentu Europejskiego.

² Publikacja dostępna pod adresem:

http://panoptykon.org/sites/panoptykon.org/files/panoptykon_safe_harbour_20.09.2013_0.pdf.

Nasze postulaty:

- Eurodeputowani powinni konsekwentnie domagać się od Komisji Europejskiej, by rozmowy dotyczące TTIP były prowadzone w sposób przejrzysty i zrozumiały dla obywateli.
- TTIP powinno respektować istniejące gwarancje ochrony praw człowieka w Unii Europejskiej. Jednocześnie w porozumieniu nie powinny być regulowane żadne kwestie, które bezpośrednio wpływają na sytuację prawną osób fizycznych.
- Przewidziany w porozumieniu mechanizm rozstrzygania sporów pomiędzy państwami i inwestorami (ISDS) powinien albo zostać gruntownie przebudowany albo wykreślony, ponieważ w obecnym kształcie zagraża podstawowym zasadom praworządności.
- W przypadku, gdy w umowie ostatecznie znajdą się rozwiązania zagrażające europejskiemu standardowi ochrony praw podstawowych, Parlament Europejski powinien sprzeciwić się jej podpisaniu.

6) Nadzór nad granicami i imigrantami

W minionej kadencji Parlament Europejski przyjął projekty zagrażające ochronie praw i wolności imigrantów. Wśród nich znalazł się m.in. kontrowersyjny system Eurosur, umożliwiający ścisły nadzór nad zewnętrznymi granicami Unii Europejskiej. Europosłowie rozpoczęli również prace nad tzw. pakietem inteligentnych granic. W ramach pakietu zostanie utworzona gigantyczna baza danych o wszystkich cudzoziemcach wjeżdżających na teren Unii Europejskiej. Projekt jednogłośnie skrytykowały organizacje pozarządowe i instytucje zajmujące się ochroną praw podstawowych, w tym Europejski Inspektor Ochrony Danych Osobowych.

Nasze postulaty:

- Parlament Europejski powinien zablokować przyjęcie pakietu inteligentnych granic – nie tylko będzie on stanowił poważne obciążenie dla budżetu Unii Europejskiej, ale przede wszystkim naruszy podstawowe standardy ochrony praw człowieka.
- Europosłowie powinni popierać tylko te rozwiązania prawne, które przyczynią się do faktycznej poprawy sytuacji cudzoziemców, a jednocześnie nie będą prowadzić do kryminalizacji i łamania praw imigrantów oraz azylantów.

7) Bezpieczeństwo w Unii Europejskiej

W 2014 r. Komisja Europejska rozpoczęła prace nad rewizją swojej strategii dotyczącej obszaru wolności, sprawiedliwości i bezpieczeństwa. Obecnie obowiązujący dokument – tzw. Program Sztokholmski – jest szeroko krytykowany przez środowiska broniące praw i wolności obywatelskich. Wśród pojawiających się zarzutów znalazły się oskarżenia o zwiększenie kompetencji służb i policji, przy jednoczesnym – nieproporcjonalnym – ograniczeniu praw podstawowych. Krytyka europejskiej polityki bezpieczeństwa płynie z różnych ośrodków, również ze strony sądów. W kwietniu br. Trybunał Sprawiedliwości Unii Europejskiej uznał za nieważną dyrektywę wprowadzającą obowiązek gromadzenia i udostępniania danych telekomunikacyjnych na potrzeby walki z przestępczością.

Niejako wbrew tej tendencji, od 2013 r. Komisja Europejska promuje szerokie wykorzystywanie dronów – czyli bezzałogowych statków powietrznych – do zapewnienia bezpieczeństwa wewnętrznego w Europie. Ten trend budzi bardzo poważne wątpliwości ze względu na naruszenia prywatności, jakie muszą się wiązać z popularyzacją dronów w charakterze standardowego środka nadzoru.

Nasze postulaty:

- Parlament Europejski powinien dołożyć wszelkich starań, by przyszła strategia dotycząca obszaru wolności obywatelskich, sprawiedliwości i bezpieczeństwa zapewniała wysoki standard ochrony praw człowieka w Unii Europejskiej.
- Europosłowie powinni sprzeciwić się wszelkim propozycjom, które miałyby na celu ponowne wprowadzenie obowiązku gromadzenia danych telekomunikacyjnych .
- Szerokie wykorzystanie dronów w europejskiej przestrzeni powietrznej budzi poważne wątpliwości z perspektywy ochrony prawa człowieka. Europosłowie powinni zainicjować poważną debatę publiczną na tematów zasad użycia dronów i ich wpływu na prawa podstawowe.

O Fundacji Panoptykon

Fundacja Panoptykon powstała w kwietniu 2009 r. Jej celem jest działanie na rzecz ochrony praw człowieka w kontekście rozwoju „społeczeństwa nadzorowanego” – współczesnych form kontroli i nadzoru nad społeczeństwem. W obszarze zainteresowania Fundacji znajdują się takie zagadnienia jak: powstawanie i rozbudowa baz danych, rozwój monitoringu wizyjnego, retencja danych telekomunikacyjnych, wykorzystywanie technologii biometrycznych, uprawnienia służb specjalnych, techniki nadzoru nad pracownikami, praktyki kontroli przepływu informacji w Internecie.