

Parlament Europejski przeciwko inwigilacji – 6 miesięcy później

Mija 6 miesięcy od przyjęcia przez Parlament Europejski rezolucji w sprawie inwigilacji, podsumowującej trwające wiele miesięcy dochodzenie w zakresie prowadzonych przez Agencję Bezpieczeństwa Narodowego (NSA) programów masowej inwigilacji oraz współpracy służb specjalnych niektórych państw Unii Europejskiej z ich amerykańskimi odpowiednikami. 11 września – z okazji Międzynarodowego Dnia Sprzeciwu Wobec Inwigilacji obchodzonego pod hasłem „Wolność a nie strach” (Freedom Not Fear Day) – Fundacja Panoptykon wzywa eurodeputowanych do podjęcia konkretnych działań na rzecz wdrożenia zawartych w rezolucji rekomendacji.

Rezolucja Parlamentu Europejskiego z 12 marca 2014 r.

Parlament Europejski poprzedniej kadencji 12 marca 2014 r. przyjął **rezolucję w sprawie amerykańskich programów masowej inwigilacji**¹. Jej kluczowym elementem jest osiem rekomendacji zebranych w akcie „**Habeas corpus w europejskiej przestrzeni cyfrowej – ochrona praw podstawowych w epoce cyfrowej**”. Rezolucja rekomenduje również dalsze działania, które instytucje oraz państwa członkowskie powinny podjąć w celu ograniczenia masowej inwigilacji i zwiększenia nadzoru nad służbami specjalnymi. Rezolucja przypomina również, że Parlament Europejski powinien odgrywać rolę strażnika praw obywateli Unii Europejskiej w epoce cyfrowej.

Zadania dla Parlamentu Europejskiego

W oparciu o ogólne rekomendacje zawarte w rezolucji, wskazujemy, jakie działania mogą podjąć eurodeputowani w obecnej kadencji Parlamentu Europejskiego, by zapewnić ich skuteczną implementację w pięciu kluczowych obszarach:

1) **Reforma przepisów o ochronie danych osobowych**

- Eurodeputowani powinni aktywnie śledzić proces negocjacji między unijnymi instytucjami (tzw. trilogu) oraz pełnić funkcję kontrolną wobec działań podejmowanych przez wyznaczonego przez parlament 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 utrzymanie gwarancji ochrony praw obywateli przynajmniej na poziomie przyjętym przez Parlament Europejski.
- Parlament Europejski powinien wywierać nacisk na rządy krajowe oraz Radę Unii Europejskiej, by prace nad reformą były prowadzone sprawnie, zapewniając szybkie

¹ Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych ([2013/2188\(INI\)](http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+Vo//PL)), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+Vo//PL>.

przyjęcie dobrych rozwiązań prawnych.

2) Umowa pomiędzy Unią Europejską a Stanami Zjednoczonymi w sprawie ochrony danych osobowych do celów egzekwowania prawa – tzw. umowa parasolowa

- Eurodeputowani powinni zadbać o zwiększenie przejrzystości procesu negocjacyjnego. W tym celu mogą zwracać się do Komisji Europejskiej z interpelacjami dotyczącymi przedmiotu umowy, przewidywanego terminu zakończenia negocjacji oraz problematycznych zagadnień;
- Eurodeputowani powinni sprzeciwić się przyjęciu tekstu umowy, jeśli zostaną utrzymane szerokie wyłączenia od zasad ochrony danych dla względów bezpieczeństwa. Przyjęcie tekstu z tak szerokimi wyłączeniami byłoby sprzeczne z podstawowym celem zawarcia takiej umowy – zwiększeniem i ujednoczeniem gwarancji ochrony praw obywateli.

3) Safe Harbour oraz porozumienia w sprawie danych PNR i SWIFT

- Eurodeputowani powinni domagać się przeprowadzenia przez Komisję Europejską pogłębionej oceny wpływu tych porozumień na poziom ochrony danych osobowych obywateli Unii Europejskiej. W przypadku negatywnej oceny, Parlament Europejski powinien żądać zawieszenia porozumień do czasu wyjaśnienia wątpliwości i przyjęcia środków naprawczych;
- Parlament Europejski powinien na bieżąco monitorować skuteczność mechanizmów ochrony praw Europejczyków, które funkcjonują w ramach konkretnych porozumień.

4) Zatwierdzenie następnego składu Komisji Europejskiej

- Zalecenia przyjęte w rezolucji z 12 marca 2014 r. powinny stanowić punkt wyjścia do dyskusji na temat masowej inwigilacji w procesie przesłuchiwania kandydatów na członków Komisji Europejskiej. Przed ostatecznym zatwierdzeniem kandydatów, eurodeputowani powinni zweryfikować ich poglądy w tej materii. Wybór komisarzy, którzy poważnie traktują ochronę praw człowieka, będzie mieć zasadniczy wpływ na dalsze wdrażanie rekomendacji.

5) Prace zespołu śledczego komisji LIBE oraz za kontrola nad wdrażaniem rezolucji z 12 marca 2014 r.

- Eurodeputowani, w szczególności wchodzący w skład komisji LIBE, powinni naciskać na utworzenie, przy komisji LIBE, specjalnej grupy monitorującej. Jej zadaniem będzie śledzenie nowych doniesień dotyczących masowej inwigilacji i kontrolowanie wdrażania rekomendacji zawartych w rezolucji z 12 marca 2014 r.;
- Eurodeputowani powinni zadbać o przejrzystość działań grupy monitoringowej oraz stałe informowanie opinii publicznej o stanie realizacji rekomendacji.

Jeśli Parlament Europejski nie podejmie problemu masowej inwigilacji obywateli, po raz kolejny ochrona praw podstawowych Europejczyków zejdzie na dalszy plan wobec potrzeby utrzymania dobrych relacji politycznych i gospodarczych ze Stanami Zjednoczonymi.

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 systemów monitoringu wizyjnego, wykorzystywanie danych telekomunikacyjnych dla celów bezpieczeństwa, uprawnienia służb specjalnych, wykorzystywanie technologii biometrycznych czy kontrolowanie przepływu informacji w Internecie.