
Od: Mikołaj Gołębiewski
Wysłano: poniedziałek, 20 lipca 2026 13:52
Do: petycje
Temat: Petycja – sprzeciw wobec wdrażania systemów firmy Palantir Technologies w strukturach Sił Zbrojnych RP
Załączniki: PETYCJA OBYWATELSKA w sprawie sprzeciwu wobec wdrażania systemów firmy Palantir Technologies w strukturach Sił Zbrojnych RP i administracji państwowej.pdf

Szanowni Państwo,

W załączeniu przesyłam petycję obywatelską skierowaną do Prezydenta Rzeczypospolitej Polskiej, Pana Karola Nawrockiego, w sprawie sprzeciwu wobec wdrażania systemów firmy Palantir Technologies w strukturach Sił Zbrojnych RP i administracji państwowej.

Dokument został opatrzony podpisem zaufanym zgodnie z wymogami Ustawy z dnia 11 lipca 2014 r. o petycjach.

Uprzejmie proszę o potwierdzenie odbioru niniejszej wiadomości oraz nadanie sprawie właściwego biegu.

Z poważaniem,
Mikołaj Gołębiewski

Wnoszący petycję:
Mikołaj Gołębiowski



PODPIS ZAUFANY

MIKOŁAJ
GOŁĘBIOWSKI
20.07.2026 13:47:07 GMT+0200
Dokument podpisany elektronicznie
podpisem zaufanym

Adresat petycji:

Szanowny Pan
Karol Nawrocki
Prezydent Rzeczypospolitej Polskiej
Kancelaria Prezydenta RP
ul. Wiejska 10
00-902 Warszawa

PETYCJA OBYWATELSKA

w sprawie sprzeciwu wobec wdrażania systemów firmy Palantir Technologies w strukturach Sił Zbrojnych RP i administracji państwowej

Działając na podstawie art. 63 Konstytucji Rzeczypospolitej Polskiej oraz art. 2 ustawy z dnia 11 lipca 2014 r. o petycjach (Dz.U. z 2018 r. poz. 870), w interesie publicznym, zwracam się do Pana Prezydenta - jako najwyższego przedstawiciela Rzeczypospolitej Polskiej oraz Zwierzchnika Sił Zbrojnych RP - z apelem o:

1. Podjęcie zdecydowanych działań w celu wstrzymania i rewizji planów wdrażania oprogramowania oraz systemów analizy danych firmy Palantir Technologies Inc. w Siłach Zbrojnych RP, w tym w strukturach Wojsk Obrony Cyberprzestrzeni, w nawiązaniu do listu intencyjnego podpisanego przez Ministerstwo Obrony Narodowej w dniu 27 października 2025 r.
2. Zwołanie Rady Bezpieczeństwa Narodowego w celu debaty nad suwerennością technologiczną i informacyjną państwa polskiego oraz ryzykiem powierzenia krytycznych zasobów informacyjnych obronności podmiotom zagranicznym.
3. Inicjatywę na rzecz stworzenia krajowych, suwerennych systemów analitycznych i sztucznej inteligencji opartych na polskich i europejskich technologiach typu otwartoźródłowego, wolnych od ryzyka zewnętrznej inwigilacji i uzależnienia od monopolu technologicznych.

Uzasadnienie

Podpisanie w październiku 2025 r. przez Ministerstwo Obrony Narodowej listu intencyjnego z amerykańską korporacją Palantir Technologies Inc. budzi głęboki niepokój społeczny i rodzi fundamentalne pytania o suwerenność cyfrową oraz bezpieczeństwo narodowe Rzeczypospolitej Polskiej.

Bazy danych i informacje, jak słusznie zauważył wicepremier Władysław Kosiniak-Kamysz podczas podpisania tego dokumentu, są „największą walutą i skarbem współczesnego świata”. Właśnie z tego powodu ich ochrona powinna opierać się na pełnej suwerenności i kontroli państwa polskiego. Przekazywanie i integrowanie krytycznych danych operacyjnych, logistycznych oraz wywiadowczych Wojska Polskiego w ramach oprogramowania dostarczanego przez podmiot powiązany z obcymi służbami wywiadowczymi wiąże się z ryzykiem. Poniżej chciałbym przytoczyć kilka punktów które uważam za najważniejsze:

1. Doświadczenia innych państw europejskich i odwrót od Palantir:

Polska nie powinna popełniać błędów, z których inne kluczowe państwa europejskie właśnie się wycofują. Flagowym przykładem jest Francja, której wywiad wewnętrzny podjął oficjalną decyzję o zakończeniu współpracy z firmą Palantir Technologies i zastąpieniu jej systemów rozwiązaniem europejskim. Na analogiczny krok i wybór europejskiej alternatywy zdecydowały się również niemieckie służby wywiadowcze. Decyzje te jasno pokazują, że czołowe gospodarki i potęgi

wywiadowcze Europy definiują obecność technologii Palantir w strukturach bezpieczeństwa państwa jako bezpośrednie zagrożenie dla własnej suwerenności.

2. Utrata suwerenności cyfrowej i uzależnienie technologiczne:

Wdrożenie systemów Palantir głęboko integruje się z infrastrukturą państwową. Wybór tej technologii skazuje Polskę na długofalowe uzależnienie od jednego, prywatnego dostawcy zagranicznego, uniemożliwiając rozwój własnych, krajowych systemów i skazując nasz kraj na cyfrowy dyktat obcego podmiotu.

3. Ryzyko geopolitycznego szantażu i nagłego odcięcia dostępu na żądanie rządu USA: Palantir

Technologies Inc. jest podmiotem amerykańskim i jako taki podlega pełnej jurysdykcji Stanów Zjednoczonych. Oznacza to, że w przypadku jakichkolwiek przyszłych rozbieżności w celach geopolitycznych między Warszawą a Waszyngtonem, rząd USA ma prawne i techniczne instrumenty, by nakazać firmie Palantir natychmiastowe ograniczenie, zablokowanie lub całkowite wyłączenie dostępu do systemów analitycznych wykorzystywanych przez Siły Zbrojne RP. Oparcie kluczowych systemów zarządzania polem walki i logistyki na technologii, którą obce mocarstwo może wyłączyć jednym dekretem administracyjnym, stanowi bezpośrednie zagrożenie dla ciągłości dowodzenia i suwerenności operacyjnej Wojska Polskiego. Ostatnia sytuacja, w której rząd USA zabronił firmie Anthropic udostępniania swojego modelu AI najlepiej to prezentuje.

4. Ryzyko inwigilacji i niekontrolowanego wycieku danych:

Palantir to firma o kontrowersyjnej reputacji, ściśle powiązana z amerykańskimi agencjami wywiadowczymi. Powierzenie takiemu podmiotowi integracji danych operacyjnych i logistycznych Wojska Polskiego stwarza realne ryzyko, że wrażliwe informacje o obronności RP będą de facto analizowane i kontrolowane poza granicami naszego kraju, bez realnego nadzoru polskich służb, parlamentu i sądów.

5. Prawa obywatelskie i nadzór algorytmiczny:

Narzędzia predykcyjne i analityczne Palantir były wielokrotnie krytykowane na świecie za naruszanie prywatności obywateli oraz brak transparentności działań algorytmów. Standardy demokratycznego państwa prawnego wymagają, aby systemy mające wpływ na bezpieczeństwo obywateli były w pełni transparentne i kontrolowalne przez czynniki społeczne i państwowe.

Polska posiada wybitnych specjalistów w dziedzinie kryptologii, cyberbezpieczeństwa i sztucznej inteligencji. Potencjał ten powinien być wykorzystany do budowy własnych, narodowych systemów bezpieczeństwa informacji lub we współpracy z partnerami europejskimi w ramach UE, a nie do zakupu licencji od amerykańskich korporacji wywiadowczych.

W związku z powyższym jako obywatel dbający o niepodległość i bezpieczeństwo Rzeczypospolitej Polskiej, proszę Pana Prezydenta o pilną interwencję w tej sprawie i podjęcie kroków uniemożliwiających monopolizację polskiej cyberprzestrzeni obronnej przez podmioty trzecie.

Z wyrazami szacunku

Mikołaj Gołębiewski