

DECYZJE

DECYZJA PARLAMENTU EUROPEJSKIEGO (UE) 2022/480

z dnia 10 marca 2022 r.

w sprawie powołania komisji śledczej w celu zbadania stosowania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego inwigilacji oraz określenia przedmiotu dochodzenia, a także zakresu odpowiedzialności, składu liczbowego i czasu trwania mandatu komisji

PARLAMENT EUROPEJSKI,

- uwzględniając wniosek złożony przez 290 posłów w sprawie powołania komisji śledczej w celu zbadania zarzutów naruszenia prawa Unii lub niewłaściwego administrowania w jego stosowaniu w odniesieniu do używania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego inwigilacji, instalowanego na urządzeniach mobilnych poprzez wykorzystanie luk informatycznych („równoważne oprogramowanie szpiegowskie”),
- uwzględniając wniosek Konferencji Przewodniczących,
- uwzględniając art. 226 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE),
- uwzględniając decyzję 95/167/WE, Euratom, EWWiS Parlamentu Europejskiego, Rady i Komisji z dnia 19 kwietnia 1995 r. w sprawie szczegółowych przepisów regulujących egzekwowanie przez Parlament Europejski jego prawa do prowadzenia dochodzeń ⁽¹⁾,
- uwzględniając przywiązanie Unii Europejskiej do wartości i zasad wolności, demokracji oraz poszanowania praw człowieka i podstawowych wolności oraz praworządności, jak określono w preambule Traktatu o Unii Europejskiej (TUE), a w szczególności w art. 2, 6 i 21 tego traktatu,
- uwzględniając art. 4 ust. 2 TUE, który potwierdza wyłączną kompetencję państw członkowskich w zakresie utrzymania porządku publicznego i ochrony bezpieczeństwa narodowego,
- uwzględniając art. 16 i 223 TFUE,
- uwzględniając Kartę praw podstawowych Unii Europejskiej (zwana dalej „Kartą”), w szczególności jej art. 7, 8, 11, 21 i 47, w których uznaje się określone w niej prawa, wolności i zasady, takie jak poszanowanie życia prywatnego i rodzinnego oraz ochrona danych osobowych, wolność wypowiedzi i informacji, prawo do niedyskryminacji, a także prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, i które mają pełne zastosowanie do państw członkowskich przy wdrażaniu prawa Unii, a także jej art. 52 ust. 1, który dopuszcza pewne ograniczenia w korzystaniu z podstawowych praw i wolności,
- uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) ⁽²⁾,
- uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ⁽³⁾,
- uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającą decyzję ramową Rady 2008/977/WSiSW ⁽⁴⁾,

⁽¹⁾ Dz.U. L 113 z 19.5.1995, s. 1.

⁽²⁾ Dz.U. L 201 z 31.7.2002, s. 37.

⁽³⁾ Dz.U. L 119 z 4.5.2016, s. 1.

⁽⁴⁾ Dz.U. L 119 z 4.5.2016, s. 89.

- uwzględniając decyzję Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim ⁽⁵⁾, zmienioną decyzją Rady (WPZiB) 2021/796 z dnia 17 maja 2021 r. ⁽⁶⁾,
- uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 z dnia 20 maja 2021 r. ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania ⁽⁷⁾,
- uwzględniając Akt dotyczący wyborów przedstawicieli do Parlamentu Europejskiego w powszechnych wyborach bezpośrednich ⁽⁸⁾,
- uwzględniając Konwencję o ochronie praw człowieka i podstawowych wolności, w szczególności jej art. 8, 9, 13 i 17, oraz protokoły do tej konwencji,
- uwzględniając Wytyczne ONZ dotyczące biznesu i praw człowieka ⁽⁹⁾,
- uwzględniając swoją rezolucję 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 ⁽¹⁰⁾, a także swoje zalecenia dotyczące wzmocnienia bezpieczeństwa informatycznego w instytucjach, organach i agencjach UE,
- uwzględniając art. 208 Regulaminu,

A. mając na uwadze niedawne doniesienia, że kilka krajów, w tym państwa członkowskie, wykorzystywało oprogramowanie szpiegowskie Pegasus do inwigilacji dziennikarzy, polityków, funkcjonariuszy organów ścigania, dyplomatów, prawników, przedsiębiorców, działaczy organizacji społeczeństwa obywatelskiego i innych podmiotów oraz że takie praktyki są niezwykle niepokojące i wydają się potwierdzać zagrożenia związane z nadużywaniem technologii inwigilacji do podważania praw człowieka i demokracji;

1. podejmuje decyzję o powołaniu komisji śledczej w celu zbadania zarzutów naruszenia prawa Unii lub niewłaściwego administrowania w jego stosowaniu w odniesieniu do używania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego, bez uszczerbku dla właściwości sądów krajowych lub unijnych;
2. postanawia, że komisja śledcza będzie miała za zadanie:
 - zbadać zakres zarzutów naruszenia prawa Unii lub niewłaściwego administrowania w jego stosowaniu, wynikających z używania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego, gromadzić informacje na temat zakresu, w jakim państwa członkowskie, w tym między innymi Węgry i Polska, lub państwa trzecie stosują natrętną inwigilację w sposób naruszający prawa i wolności zapisane w Karcie, a także ocenić poziom ryzyka, jakie stanowi to dla wartości zapisanych w art. 2 TUE, takich jak demokracja, praworządność i poszanowanie praw człowieka;
 - na potrzeby wykonywania swoich obowiązków – gromadzić i analizować informacje w celu potwierdzenia:
 - stosowania i funkcjonowania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego oraz jego domniemanego negatywnego wpływu na prawa podstawowe zapisane w Karcie w przypadkach, w których państwa członkowskie wdrażały prawo Unii;
 - obowiązujących ram prawnych, w których państwa członkowskie nabyły i stosowały oprogramowanie Pegasus i równoważne oprogramowanie szpiegowskie;
 - czy organy państw członkowskich korzystały z oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego do celów politycznych, gospodarczych lub innych nieuzasadnionych celów inwigilacji dziennikarzy, polityków, funkcjonariuszy organów ścigania, dyplomatów, prawników, przedsiębiorców, działaczy organizacji społeczeństwa obywatelskiego lub innych podmiotów, co stanowi naruszenie prawa Unii i wartości zapisanych w art. 2 TUE lub praw zapisanych w Karcie;

⁽⁵⁾ Dz.U. L 129 I z 17.5.2019, s. 13.

⁽⁶⁾ Dz.U. L 174 I z 18.5.2021, s. 1.

⁽⁷⁾ Dz.U. L 206 z 11.6.2021, s. 1.

⁽⁸⁾ Dz.U. L 278 z 8.10.1976, s. 5.

⁽⁹⁾ https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

⁽¹⁰⁾ Dz.U. C 378 z 9.11.2017, s. 104.

- czy stosowanie oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego wbrew prawu Unii miało negatywny wpływ na procesy demokratyczne w państwach członkowskich dotyczące wyborów na szczeblu lokalnym, krajowym i europejskim;
- zarzutów naruszenia dyrektywy 2002/58/WE lub niewłaściwego administrowania w jej stosowaniu przez państwa członkowskie, wynikających z używania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego, w szczególności w odniesieniu do zasady poufności komunikacji oraz zakazu słuchania, nagrywania, przechowywania lub innych rodzajów przejścia lub nadzoru komunikatu i związanych z nim danych o ruchu osób;
- czy stosowanie oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego przez państwa członkowskie stanowiło naruszenie dyrektywy (UE) 2016/680 i rozporządzenia (UE) 2016/679, doprowadziło do takich naruszeń lub je ujawniło;
- czy Komisja posiadała dowody na stosowanie oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego przeciwko osobom;
- czy państwa członkowskie zadbały o wystarczające zabezpieczenia instytucjonalne i prawne, aby uniknąć nielegalnego korzystania z oprogramowania szpiegowskiego, oraz czy osoby, które podejrzewają, że ich prawa zostały naruszone przez stosowanie oprogramowania szpiegowskiego, mają dostęp do skutecznego środka odwoławczego;
- domniemanego niepodejmowania przez państwa członkowskie działań w odniesieniu do zaangażowania podmiotów w UE w opracowywanie, rozpowszechnianie lub finansowanie oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego, w tym łańcucha dostaw pod względem technologii i jej wykorzystania, w zakresie, w jakim narusza to prawo Unii, w tym rozporządzenie (UE) 2021/821, w tym w przypadku, gdy oprogramowanie szpiegowskie wprowadzane do obrotu w określonym celu (np. walka z terroryzmem) jest wykorzystywane w innym kontekście;
- roli rządu Izraela i innych państw trzecich w dostarczaniu państwom członkowskim oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego;
- czy stosowanie oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego przez organy państw członkowskich doprowadziło do przekazania danych osobowych państwom trzecim, w szczególności m.in. grupie NSO, a także rządów państw trzecich;
- czy stosowanie oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego z bezpośrednim lub pośrednim udziałem podmiotów powiązanych z UE przyczyniło się do nielegalnego szpiegowania dziennikarzy, polityków, funkcjonariuszy organów ścigania, dyplomatów, prawników, przedsiębiorców, organizacji społeczeństwa obywatelskiego lub innych podmiotów w państwach trzecich oraz czy doprowadziło do łamania lub naruszeń praw człowieka budzących poważne obawy w odniesieniu do celów wspólnej polityki zagranicznej i bezpieczeństwa UE oraz czy stosowanie takiego oprogramowania było sprzeczne z wartościami zapisanymi w art. 21 TUE i w Karcie praw podstawowych, a także z należyтым uwzględnieniem Wytocznych ONZ dotyczących biznesu i praw człowieka oraz innych praw zapisanych w międzynarodowym prawie dotyczącym praw człowieka;
- czy istniały wystarczające podstawy do przyjęcia przez Radę środków ograniczających lub sankcji w ramach wspólnej polityki zagranicznej i bezpieczeństwa UE wobec jednego lub większej liczby państw trzecich, w przypadku gdy decyzja przyjęta zgodnie z tytułem V rozdział 2 TUE przewidywała zerwanie lub ograniczenie stosunków gospodarczych lub finansowych, zgodnie z art. 215 ust. 1 TFUE;
- czy stosowanie oprogramowania Pegasus lub równoważnego oprogramowania szpiegowskiego przez państwa trzecie miało wpływ na prawa podstawowe zagwarantowane w prawie Unii oraz czy istnieją wystarczające podstawy, by Rada dokonała ponownej oceny wszelkich umów o współpracy międzynarodowej w przestrzeni wolności, bezpieczeństwa i sprawiedliwości zawartych z państwami trzecimi zgodnie z art. 218 TFUE;
- przedstawić wszelkie zalecenia, jakie uzna za niezbędne w tym względzie;
- przedstawić zalecenia dotyczące ochrony instytucji UE, jej członków i pracowników przed takim oprogramowaniem szpiegowskim;

3. postanawia, że komisja śledcza przedstawi sprawozdanie końcowe w terminie 12 miesięcy od momentu przyjęcia niniejszej decyzji;
 4. postanawia, że komisja śledcza powinna uwzględnić w swoich pracach wszelkie istotne zmiany dotyczące kwestii należących do jej kompetencji, które to zmiany wystąpią w czasie trwania jej mandatu;
 5. podkreśla, że w celu zapewnienia dobrej współpracy i przepływu informacji między komisją śledczą a właściwymi komisjami stałymi i podkomisjami przewodniczący i sprawozdawca komisji śledczej mogą być zaangażowani w odpowiednie debaty komisji stałych i podkomisji i odwrotnie, w szczególności w przypadku wysłuchań komisji śledczej;
 6. postanawia, że zalecenia wydane przez komisję śledczą powinny być przekazywane odpowiednim stałym komisjom i podkomisjom w obszarach ich kompetencji określonych w załączniku VI do Regulaminu;
 7. postanawia, że komisja śledcza będzie liczyć 38 członków;
 8. zobowiązuje swoją przewodniczącą do zapewnienia publikacji niniejszej decyzji w *Dzienniku Urzędowym Unii Europejskiej*.
-