



P9_TA(2023)0440

Niepodjęcie działań legislacyjnych przez Komisję w następstwie rezolucji w sprawie oprogramowania Pegasus

Rezolucja Parlamentu Europejskiego z dnia 23 listopada 2023 r. w sprawie niepodjęcia działań legislacyjnych przez Komisję w następstwie rezolucji w sprawie oprogramowania Pegasus (2023/2988(RSP))

(C/2024/4226)

Parlament Europejski,

- uwzględniając art. 13 ust. 2 Traktatu o Unii Europejskiej i zasadę lojalnej współpracy,
 - uwzględniając porozumienie ramowe z dnia 20 listopada 2010 r. w sprawie stosunków między Parlamentem Europejskim i Komisją Europejską ⁽¹⁾,
 - uwzględniając porozumienie międzyinstytucjonalne z dnia 13 kwietnia 2016 r. zawarte pomiędzy Parlamentem Europejskim, Radą Unii Europejskiej a Komisją Europejską w sprawie lepszego stanowienia prawa ⁽²⁾,
 - uwzględniając sprawozdanie z dnia 22 maja 2023 r. sporządzone przez parlamentarną komisję śledczą ds. zbadania stosowania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego inwigilacji (A9-0189/2023),
 - uwzględniając swoje zalecenie z dnia 15 czerwca 2023 r. dla Rady i Komisji w następstwie dochodzenia w sprawie zarzutów naruszenia prawa Unii i niewłaściwego administrowania w jego stosowaniu w odniesieniu do oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego ⁽³⁾,
 - uwzględniając art. 208 ust. 13 Regulaminu,
 - uwzględniając art. 132 ust. 2 Regulaminu,
- A. mając na uwadze, że 15 czerwca 2023 r. Parlament przyjął zalecenie dla Rady i Komisji w następstwie dochodzenia w sprawie zarzutów naruszenia prawa Unii i niewłaściwego administrowania w jego stosowaniu w odniesieniu do oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego, które to zalecenie zawierało wnioski dotyczące działań legislacyjnych i nielegislacyjnych na szczeblu UE w celu uregulowania stosowania oprogramowania szpiegującego, co miało chronić prawa Unii i prawa zapisane w Karcie praw podstawowych Unii Europejskiej;
- B. mając na uwadze, że porozumienie ramowe i porozumienie międzyinstytucjonalne w sprawie lepszego stanowienia prawa zobowiązują Komisję do udzielenia odpowiedzi na wnioski dotyczące działań Unii złożone przez Parlament w terminie trzech miesięcy, wraz z określeniem działań następczych, jakie zamierza podjąć w związku z tymi wnioskami;
- C. mając na uwadze, że ponad pięć miesięcy po przyjęciu zalecenia Komisja nie przekazała Parlamentowi formalnej odpowiedzi przedstawiającej podjęte działania i plany na przyszłość;
- D. mając na uwadze, że od czasu przyjęcia zalecenia Parlamentu w UE zgłoszono nowe przypadki nadużyć związanych z oprogramowaniem szpiegującym, na które nie zareagowały ani władze krajowe, ani Komisja;
- E. mając na uwadze, że afera „Predator files” ujawniła, iż posłowie do Parlamentu Europejskiego, w tym przewodnicząca Roberta Metsola i Pierre Karleskind, a także urzędnicy Komisji i inne osoby, byli celem ataków z wykorzystaniem oprogramowania szpiegującego Predator; mając na uwadze, że doniesienia medialne wskazują, iż ataki nastąpiły z państw trzecich;
- F. mając na uwadze, że ujawniono, iż telefon rosyjskiej dziennikarki Galiny Timczenko, która przebywa na wygnaniu, został zainfekowany oprogramowaniem szpiegującym Pegasus podczas jej pobytu w Niemczech;
- G. mając na uwadze doniesienia, że telefon egipskiego kandydata na prezydenta Ahmeda Tantawy'ego był wielokrotnie hakowany przy użyciu oprogramowania szpiegującego Predator, sprzedawanego przez europejską firmę Intellexa;

⁽¹⁾ Dz.U. L 304 z 20.11.2010, s. 47.

⁽²⁾ Dz.U. L 123 z 12.5.2016, s. 1.

⁽³⁾ Teksty przyjęte, P9_TA(2023)0244.

- H. mając na uwadze, że Grecki Urząd ds. Bezpieczeństwa Komunikacji i Prywatności (ADAE) oraz Urząd Ochrony Danych zidentyfikowały 92 osoby inwigilowane w Grecji, prokuratorzy prowadzący sprawę zwrócili się o porównanie tej listy z osobami objętymi nadzorem przez greckie służby wywiadowcze (EYP), prokuratorzy postawili zarzuty karne dwóm urzędnikom EYP, a następnie zarząd ADAE stanął w obliczu nagłych zmian i akta zostały przekazane innemu prokuratorowi;
- I. mając na uwadze, że sędzia prowadzący sprawę w Hiszpanii tymczasowo zawiesił dochodzenie w sprawie domniemych ataków szpiegowskich Maroka na premiera i ministrów rządu z powodu braku współpracy ze strony władz Izraela;
- J. mając na uwadze, że ujawniono, iż francuska firma Nexa Technologies sprzedawała oprogramowanie szpiegujące Predator represyjnym reżimom, w tym Egiptowi, Wietnamowi i Madagaskarowi;
- K. mając na uwadze, że żadne ze sprawozdań, częściowo udokumentowanych w zaleceniach Parlamentu, zarzucających Intellexie i innym przedsiębiorstwom możliwe naruszenie rozporządzenia w sprawie produktów podwójnego zastosowania (*) nie doprowadziło do podjęcia wiarygodnych działań następczych przez organy krajowe lub Komisję; mając na uwadze, że brak kontroli może nadal stwarzać sprzyjające warunki dla podmiotów działających w złym zamiarze w tej dziedzinie;
- L. mając na uwadze, że 6 września 2023 r. komisja nadzwyczajna Senatu RP do spraw wyjaśnienia przypadków nielegalnej inwigilacji i ich wpływu na proces wyborczy przyjęła sprawozdanie końcowe, w którym stwierdziła, że w Polsce program Pegasus był wykorzystywany przeciwko osobom, przeciwko którym nie toczyło się postępowanie karne, a ofiary inwigilacji były szpiegowane z powodów politycznych;
- M. mając na uwadze, że zwrócono się do irlandzkiej Komisji Sprawiedliwości Oireachtas o zbadanie roli Intellexa Group w sprzedaży oprogramowania szpiegującego;
- N. mając na uwadze, że 18 lipca 2023 r. Departament Handlu Stanów Zjednoczonych dodał Intellexa S.A. w Grecji, Intellexa Limited w Irlandii, Cytrox Holdings Zrt. na Węgrzech i Cytrox AD w Macedonii Północnej do listy podmiotów, które dopuściły się handlu programami exploit wykorzystywanymi do uzyskiwania dostępu do systemów informatycznych, co zagraża prywatności i bezpieczeństwu osób fizycznych i organizacji na całym świecie;
- O. mając na uwadze, że duża liczba spraw dobitnie pokazała, iż istniejące ramy prawne – zarówno w niektórych państwach członkowskich, jak i na szczeblu europejskim – nie są wystarczające, aby zapobiegać nadużyciom i karać niewłaściwe wykorzystywanie szpiegowskiego oprogramowania do nadzoru;
- P. mając na uwadze, że te doniesienia wskazują na pilną potrzebę podjęcia działań przez Unię;
1. wyraża głębokie ubolewanie z powodu braku środków egzekwowania prawa i działań legislacyjnych ze strony Komisji w odpowiedzi na zalecenie Parlamentu z 15 czerwca 2023 r.; ostrzega przed lekceważeniem zagrożeń dla obywateli i demokracji w UE wynikających z nadużywania oprogramowania szpiegującego;
 2. wzywa Komisję do poszanowania zasady lojalnej współpracy między instytucjami Unii oraz do przestrzegania zobowiązań określonych w porozumieniu ramowym i porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa; wzywa pilnie Komisję, aby bez zbędnej zwłoki przedstawiła plan środków mających na celu zapobieganie nadużyciu oprogramowania szpiegującego w UE, przy pełnym wykorzystaniu wszystkich dostępnych środków ustawodawczych i nieustawodawczych przewidzianych w traktatach europejskich;
 3. przypomina swój apel do Komisji, by do 30 listopada 2023 r. oceniła spełnienie określonych w zaleceniu warunków szczegółowych dotyczących Cypru, Grecji, Węgier, Polski i Hiszpanii;
 4. zobowiązuje swoją przewodniczącą do przekazania niniejszej rezolucji Radzie i Komisji oraz rządów i parlamentom państw członkowskich.

(*) 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 (Dz.U. L 206 z 11.6.2021, s. 1).