P8_TA(2015)0388

Działania następcze w związku z rezolucją Parlamentu Europejskiego z dnia 12 marca 2014 r. dotyczącą masowego nadzoru elektronicznego wobec obywateli UE

Rezolucja Parlamentu Europejskiego z dnia 29 października 2015 r. w sprawie działań następczych w związku z rezolucją Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie masowej inwigilacji elektronicznej obywateli UE (2015/2635(RSP))

(2017/C 355/07)

Parlament Europejski,

— uwzględniając ramy prawne określone Traktatem o Unii Europejskiej (TUE), w szczególności jego art. 2, 3, 4, 5, 6, 7, 10 i 21, Kartą praw podstawowych Unii Europejskiej, w szczególności jej art. 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 i 52, europejską konwencją praw człowieka, w szczególności jej art. 6, 8, 9, 10 i 13, oraz orzecznictwem sądów europejskich dotyczącym bezpieczeństwa, ochrony prywatności i wolności wypowiedzi,

— 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 ([1]) (dalej zwaną „rezolucją"),

— uwzględniając dokument roboczy z dnia 19 stycznia 2015 r. w sprawie działań następczych w związku z dochodzeniem LIBE w sprawie masowej inwigilacji elektronicznej obywateli UE ([2]),

— uwzględniając rezolucję Zgromadzenia Parlamentarnego Rady Europy z dnia 21 kwietnia 2015 r. w sprawie masowej inwigilacji,

— uwzględniając pytania do Rady i do Komisji w sprawie działań w następstwie rezolucji Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie masowej elektronicznej inwigilacji obywateli UE (O-000114/2015 – B8–0769/2015 i O-000115/2015 – B8–0770/2015),

— uwzględniając projekt rezolucji Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych,

— uwzględniając art. 128 ust. 5 i art. 123 ust. 2 Regulaminu,

A. mając na uwadze, że w rezolucji Parlament wezwał władze USA i państwa członkowskie do wprowadzenia zakazu prowadzenia nieograniczonej inwigilacji na masową skalę i masowego przetwarzania danych osobowych obywateli oraz potępił ujawnione działania służb wywiadowczych, które stanowiły poważne nadużycie zaufania obywateli UE i rażące naruszenie ich praw podstawowych; mając na uwadze, że w rezolucji zwrócono uwagę na ewentualne inne motywy niż tylko szpiegostwo polityczne i gospodarcze, wziąwszy pod uwagę możliwości oferowane przez ujawnione programy masowej inwigilacji;

B. mając na uwadze, że w rezolucji ustanowiono akt pt. „Habeas corpus w europejskiej przestrzeni cyfrowej – ochrona praw podstawowych w epoce cyfrowej" obejmujący osiem szczegółowych działań i zobowiązano w niej Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych do zdania za rok sprawy Parlamentowi w celu dokonania oceny stopnia wdrożenia wytycznych;

C. mając na uwadze, że w dokumencie roboczym z dnia 19 stycznia 2015 r. zdano sprawę z rozwoju sytuacji od czasu przyjęcia rezolucji, jako że wciąż ujawniane są nowe fakty dotyczące domniemanej masowej inwigilacji elektronicznej, oraz ze stanu wdrożenia zaproponowanego aktu „Habeas corpus w europejskiej przestrzeni cyfrowej" ze wskazaniem na ograniczoną reakcję instytucji, państw członkowskich i zainteresowanych stron, które wezwano do działania;

([1]) Teksty przyjęte, P7_TA(2014)0230.
([2]) PE546.737v01-00.

Czwartek, 29 października 2015 r.

D. mając na uwadze, że w rezolucji Parlament wezwał Komisję i inne instytucje, organy, agencje i jednostki organizacyjne UE do działania według zaleceń zgodnie z art. 265 TFUE („zaniechanie działania”);

E. mając na uwadze, że niedawno portal WikiLeaks ujawnił ukierunkowaną inwigilację rozmów i korespondencji trzech ostatnich prezydentów Francji oraz ministrów francuskiego rządu i ambasadora Francji w USA; mając na uwadze, że przez ostatnie dziesięć lat NSA prowadziła zakrojoną na szeroką skalę strategiczną i gospodarczą działalność szpiegowską wobec wszystkich francuskich struktur państwowych i największych francuskich przedsiębiorstw;

F. mając na uwadze, że w swoim raporcie Specjalny Sprawozdawca ds. Promocji i Ochrony Prawa do Wolności Opinii i Wypowiedzi stwierdził, iż szyfrowanie i anonimowość zapewniają ochronę prywatności i bezpieczeństwo niezbędne do wykonywania prawa do wolności opinii i wypowiedzi w dobie cyfrowej; mając na uwadze, że w raporcie tym stwierdzono też, iż wszelkie działania służące ograniczaniu szyfrowania i anonimowości musi być zgodne z zasadami legalności, konieczności, proporcjonalności i zasadności;

1. przyjmuje z zadowoleniem dochodzenia przeprowadzone przez Bundestag, Radę Europy, ONZ i Senat Brazylii, debaty w kilku innych parlamentach narodowych oraz prace wielu podmiotów społeczeństwa obywatelskiego, które przyczyniły się do uświadomienia opinii publicznej istnienia masowej inwigilacji elektronicznej;

2. wzywa państwa członkowskie UE do wycofania zarzutów karnych, o ile takie zostały przedstawione, wobec Edwarda Snowdena i do zapewnienia mu ochrony oraz w związku z tym zapobiegnięcia jego ekstradycji lub wydaniu go przez osoby trzecie, w uznaniu dla jego statusu osoby zgłaszającej przypadki naruszenia i obrońcy praw człowieka na szczeblu międzynarodowym;

3. jest jednak bardzo rozczarowany tym, że większość państw członkowskich i instytucji UE nie uznała tej kwestii za pilną i nie wyraziła gotowości do poważnego potraktowania kwestii poruszonych w rezolucji oraz do zastosowania się do konkretnych zawartych w niej zaleceń, a także brakiem przejrzystości wobec Parlamentu i brakiem dialogu z Parlamentem;

4. jest zaniepokojony niektórymi niedawno przyjętymi przez niektóre państwa członkowskie ustawami, które rozszerzają zakres możliwości inwigilacji ze strony organów wywiadowczych, w tym nową ustawą przyjętą we Francji przez Zgromadzenie Narodowe dnia 24 czerwca 2015 r., której wiele przepisów – zdaniem Komisji – wzbudza poważne wątpliwości natury prawnej, przyjęciem przez Zjednoczone Królestwo w 2014 r. ustawy o zatrzymywaniu danych i uprawnieniach śledczych (DRIPA) oraz późniejszą decyzją sądu, że niektóre artykuły są niezgodne z prawem i nie mogą być stosowane, oraz projektami nowych przepisów w Holandii zmierzającymi do nowelizacji ustawy z 2002 r. o służbach wywiadowczych i służbach bezpieczeństwa; ponawia swój apel do wszystkich państw członkowskich o dopilnowanie, by ich obowiązujące i przyszłe ramy ustawodawcze oraz mechanizmy nadzoru regulujące działalność agencji wywiadowczych były zgodne z normami europejskiej konwencji praw człowieka oraz właściwym prawodawstwem unijnym;

5. z zadowoleniem przyjmuje przeprowadzone przez Bundestag dochodzenie w sprawie masowej inwigilacji; jest poważnie zaniepokojony przypadkami ujawnionej masowej inwigilacji ruchu telekomunikacyjnego i internetowego w Unii przez niemiecką agencję wywiadu BND we współpracy z NSA; uważa to za naruszenie zasady lojalnej współpracy, o której mowa w art. 4 ust. 3 TUE;

6. zwraca się do swojego przewodniczącego, by zaapelował do sekretarza generalnego Rady Europy o wszczęcie procedury z art. 52, zgodnie z którym „na żądanie Sekretarza Generalnego Rady Europy każda Wysoka Układająca się Strona złoży wyjaśnienie w sprawie sposobu, w jaki jej prawo wewnętrzne zapewnia skuteczne stosowanie wszystkich postanowień niniejszej konwencji”;

7. uważa, że dotychczasowa reakcja Komisji na rezolucję jest zupełnie nieodpowiednia, biorąc pod uwagę zakres ujawnionych faktów; wzywa Komisję do przeprowadzenia najpóźniej do grudnia 2015 r. działań, do których wezwano ją w rezolucji; zastrzega sobie prawo do złożenia skargi w sprawie zaniechania działania lub umieszczenia pewnych zasobów budżetowych Komisji w rezerwie do czasu, aż zastosuje się ona odpowiednio do wszystkich zaleceń;

8. podkreśla znaczenie wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r. stwierdzającego nieważność dyrektywy 2006/24/WE w sprawie zatrzymywania danych; przypomina, że Trybunał stwierdził, iż ingerencja w prawo podstawowe do prywatności musi się ograniczać do tego, co ściśle niezbędne; zwraca uwagę na fakt, że orzeczenie to zawiera aspekt nowatorski, ponieważ Trybunał Sprawiedliwości odnosi się konkretnie do określonego zbioru orzecznictwa Europejskiego Trybunału Praw Człowieka dotyczącego kwestii „ogólnych programów inwigilacji" i wprowadza obecnie do prawa UE w tej samej dziedzinie te same zasady, wywodzące się z tego konkretnego orzecznictwa Europejskiego Trybunału Praw Człowieka; podkreśla, że należy zatem oczekiwać, że Trybunał Sprawiedliwości w przyszłości również będzie stosował to samo rozumowanie przy ocenie ważności, w świetle Karty, innych aktów ustawodawczych UE i państw członkowskich w tej samej dziedzinie „ogólnych programów inwigilacji";

Pakiet dotyczący ochrony danych

9. z zadowoleniem przyjmuje rozpoczęcie nieformalnych negocjacji międzyinstytucjonalnych w sprawie projektu ogólnego rozporządzenia o ochronie danych oraz przyjęcie przez Radę ogólnego podejścia do projektu dyrektywy o ochronie danych; ponownie wyraża pragnienie zakończenia negocjacji nad pakietem dotyczącym ochrony danych w 2015 r.;

10. przypomina Radzie o jej zobowiązaniu do przestrzegania Karty praw podstawowych Unii Europejskiej przy formułowaniu poprawek do wniosków Komisji; w szczególności ponownie wyraża stanowisko, że oferowany poziom ochrony nie powinien być niższy niż poziom ustanowiony dyrektywą 95/46/WE;

11. podkreśla, że zarówno rozporządzenie w sprawie ochrony danych, jak i dyrektywa w sprawie ochrony danych są niezbędne do ochrony praw podstawowych osób, a zatem oba akty muszą być traktowane jako pakiet, który należy przyjąć równocześnie, aby zapewnić wysoki poziom ochrony we wszystkich okolicznościach podczas wszystkich działań związanych z przetwarzaniem danych w UE; podkreśla, że dzięki przyjęciu tego pakietu musi zostać osiągnięty cel wzmocnienia praw i ochrony jednostki w związku z przetwarzaniem jej danych osobowych;

Umowa parasolowa UE–USA

12. zauważa, że już po przyjęciu rezolucji negocjacje z USA w sprawie umowy ramowej między UE a Stanami Zjednoczonymi Ameryki o ochronie danych osobowych przekazywanych i przetwarzanych do celów egzekwowania prawa (dalej zwanej „umową parasolową") zostały zakończone i parafowano projekt umowy;

13. przyjmuje z zadowoleniem wysiłki rządu USA zmierzające do odbudowy zaufania dzięki umowie parasolowej, a ze szczególnym zadowoleniem przyjmuje fakt, że ustawa o sądowych środkach odwoławczych z 2015 r. („Judicial Redress Act of 2015") została uchwalona przez Izbę Reprezentantów w dniu 20 października 2015 r., przy czym podkreśla istotne i pozytywne kroki podjęte przez USA w celu wyjaśnienia obaw UE; uważa, że zagwarantowanie takich samych praw do skutecznych środków odwoławczych obywatelom UE/osobom, których dane osobowe są przetwarzane w UE i przekazywane USA, bez jakiejkolwiek dyskryminacji między obywatelami UE i USA w takich samych okolicznościach jest niezwykle ważne; wzywa Senat USAdo przyjęcia przepisów gwarantujących takie prawa; podkreśla, że przyjęcie przez Kongres ustawy o sądowych środkach odwoławczych jest warunkiem wstępnym podpisania i zawarcia umowy parasolowej;

Bezpieczny transfer danych osobowych

14. przypomina, że w rezolucji wezwano do bezzwłocznego zawieszenia decyzji w sprawie bezpiecznego transferu danych osobowych, gdyż nie przewiduje ona odpowiedniej ochrony danych osobowych obywateli UE;

15. przypomina, że każda umowa międzynarodowa zawarta przez UE ma pierwszeństwo przed prawem wtórnym UE; podkreśla zatem, że trzeba dopilnować, by umowa parasolowa nie ograniczała praw osób, których dane dotyczą, oraz gwarancji mających zastosowanie do przekazywania danych na mocy prawa UE; wzywa zatem Komisję, by dokładnie zbadała, jak umowa parasolowa oddziaływałaby na ramy prawne UE w dziedzinie ochrony danych i jaki miałaby na nie wpływ, w tym odpowiednio na aktualnie obowiązującą decyzję ramową Rady, dyrektywę w sprawie ochrony danych (95/46/WE) oraz przyszłą dyrektywę i rozporządzenie w dziedzinie ochrony danych; wzywa Komisję do przedstawienia Parlamentowi sprawozdania z oceny prawnej tej kwestii przed rozpoczęciem procedury ratyfikacji;

16. przypomina, że Komisja w swoim komunikacie z dnia 27 listopada 2013 r. w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych wydała pod adresem USA 13 zaleceń w celu zagwarantowania odpowiedniego poziomu ochrony;

17. przyjmuje z zadowoleniem, że w swoim wyroku z dnia 6 października 2015 r. Trybunał Sprawiedliwości Unii Europejskiej stwierdził nieważność decyzji Komisji w sprawie odpowiedniej ochrony danych osobowych 2000/520/WE dotyczącej stosowanych przez USA zasad bezpiecznego transferu danych osobowych; podkreśla, że wyrok ten potwierdził utrwalone od dawna stanowisko Parlamentu, zgodnie z którym instrument ten nie zapewnia odpowiedniego stopnia ochrony; wzywa Komisję do niezwłocznego podjęcia działań niezbędnych do zadbania o to, by wszystkie dane osobowe przekazywane do USA podlegały skutecznej ochronie na takim poziomie, który zasadniczo jest równoważny z poziomem ochrony gwarantowanym w UE;

18. potępia fakt, że Parlament nie otrzymał ze strony Komisji żadnego oficjalnego komunikatu dotyczącego stanu wdrożenia tych 13 zaleceń, choć Komisja zapowiedziała, że wyda taki komunikat do lata 2014 r.; podkreśla, że w związku z decyzją Trybunału Sprawiedliwości Unii Europejskiej o unieważnieniu decyzji 2000/520/WE Komisja powinna teraz w trybie pilnym przedstawić szczegółowe informacje o dotychczasowym przebiegu negocjacji oraz o skutkach wyroku dla zapowiedzianych dalszych rund negocjacji; zachęca Komisję do niezwłocznego zastanowienia się nad alternatywnymi rozwiązaniami dla zasad bezpiecznego transferu danych osobowych i nad skutkami wyroku dla wszelkich innych instrumentów służących przekazywaniu danych osobowych do USA oraz do przedstawienia wyników tej refleksji do końca 2015 r.;

19. wzywa Komisję do oceny wpływu i skutków prawnych wyroku Trybunału Sprawiedliwości z dnia 6 października 2015 r. w sprawie Schrems (C-362/14) dla wszelkich umów z państwami trzecimi umożliwiających przekazywanie danych osobowych, jak np. umowa między UE a USA w sprawie programu śledzenia środków należących do terrorystów (TFTP), umowa w sprawie danych dotyczących przelotu pasażera (PNR), umowa parasolowa między UE a USA i inne instrumenty na mocy prawa UE, które obejmują gromadzenie i przetwarzanie danych osobowych;

Nadzór demokratyczny

20. w pełnym poszanowaniu faktu, że parlamenty narodowe mają pełne uprawnienia do nadzorowania krajowych służb wywiadowczych, wzywa wszystkie parlamenty narodowe, które jeszcze tego nie uczyniły, do ustanowienia prawdziwego nadzoru nad działalnością wywiadowczą i do oceny tej działalności oraz do zadbania o to, by takie komisje/organy nadzorujące posiadały dostateczne zasoby, fachową wiedzę techniczną i środki prawne oraz dostęp do wszystkich odnośnych dokumentów, aby móc skutecznie i w niezależny sposób nadzorować służby wywiadowcze oraz wymianę informacji z innymi służbami wywiadowczymi; ponownie wyraża swoje zobowiązanie do ścisłej współpracy z parlamentami narodowymi na rzecz zadbania o wprowadzenie skutecznych mechanizmów nadzoru, w tym poprzez dzielenie się najlepszymi praktykami i stosowanie wspólnych norm;

21. zamierza śledzić wyniki konferencji w sprawie demokratycznego nadzoru nad służbami wywiadowczymi w Unii Europejskiej, która odbyła się w dniach 28–29 maja 2015 r., i czynić dalsze wysiłki na rzecz zapewnienia wymiany dobrych praktyk w dziedzinie nadzoru nad wywiadem w ścisłej współpracy z parlamentami narodowymi; pozytywnie ocenia wspólne uwagi końcowe współprzewodniczących tej konferencji, którzy wyrazili zamiar zwołania kolejnej konferencji za dwa lata;

22. uważa, że należy wspierać i w większym stopniu wykorzystywać istniejące narzędzia współpracy między organami nadzoru, np. europejską sieć ds. monitorowania krajowych służb wywiadowczych (ENNIR), ewentualnie poprzez wykorzystywanie potencjału platformy IPEX do wymiany informacji między parlamentami narodowymi zgodnie z jej zakresem i możliwościami technicznymi;

23. ponawia apel o zawieszenie umowy w sprawie programu śledzenia środków należących do terrorystów (TFTP);

24. podkreśla, że aby Unia Europejska i jej państwa członkowskie mogły zagwarantować pewność prawa, potrzebna jest wspólna definicja „bezpieczeństwa narodowego"; zauważa, że brak jednoznacznej definicji umożliwia arbitralność oraz naruszanie praw podstawowych i zasad praworządności przez kręgi wykonawcze i wywiadowcze w UE;

25. zachęca Komisję i państwa członkowskie do wprowadzenia do ustawodawstwa umożliwiającego gromadzenie danych osobowych lub inwigilację obywateli europejskich przepisów dotyczących wygaśnięcia i przedłużenia; podkreśla, że takie przepisy są istotnymi gwarancjami służącymi zadbaniu o to, by instrument naruszający prywatność był regularnie analizowany pod względem jego niezbędności i proporcjonalności w społeczeństwie demokratycznym;

Odbudowa zaufania

26. podkreśla, że poprawne stosunki UE–USA pozostają absolutnie kluczowe dla obojga partnerów; zauważa, że doniesienia o inwigilacji osłabiły poparcie opinii publicznej dla tych wzajemnych stosunków, oraz podkreśla, że należy podjąć działania, by zapewnić odbudowę zaufania, zwłaszcza w świetle obecnej pilnej potrzeby współpracy w zakresie wielu geopolitycznych kwestii będących przedmiotem wspólnego zainteresowania; podkreśla w związku z tym, że należy znaleźć w drodze negocjacji między USA i całą UE rozwiązanie nienaruszające praw podstawowych;

27. z zadowoleniem przyjmuje niedawne decyzje ustawodawcze i sądowe podjęte w USA w celu ograniczenia masowej inwigilacji przez NSA, takie jak przyjęcie przez Kongres bez poprawek ustawy o wolności w wyniku kompromisu między obiema izbami i partiami oraz wyrok Drugiego Okręgowego Sądu Apelacyjnego w sprawie programu gromadzenia przez NSA zapisów rozmów telefonicznych; ubolewa jednak, że decyzje te skupiają się głównie na Amerykanach, a sytuacja obywateli UE nie ulega zmianie;

28. uważa, że każda decyzja o zastosowaniu technologii inwigilacji powinna opierać się na szczegółowej ocenie konieczności i proporcjonalności; z zadowoleniem przyjmuje wyniki projektu badawczego „SURVEILLE", który oferuje metodykę dokonywania oceny technologii inwigilacji z uwzględnieniem aspektów prawnych, etycznych i technologicznych;

29. podkreśla, że UE powinna przyczynić się do opracowania na szczeblu ONZ międzynarodowych norm/zasad zgodnych z Międzynarodowym paktem praw obywatelskich i politycznych ONZ w celu stworzenia światowych ram ochrony danych, obejmujących szczegółowe ograniczenia dotyczące gromadzenia danych do celów związanych z bezpieczeństwem narodowym;

30. jest przekonany, że „wyścigu zbrojeń w zakresie inwigilacji" można będzie uniknąć tylko wtedy, gdy na szczeblu światowym zostaną ustanowione wiarygodne normy;

Przedsiębiorstwa prywatne

31. przyjmuje z zadowoleniem inicjatywy sektora ICT służące rozwojowi rozwiązań w zakresie bezpieczeństwa kryptograficznego oraz usług internetowych zapewniających lepszą ochronę prywatności; zachęca do stałego rozwijania przyjaznych dla użytkownika ustawień aplikacji pomagających konsumentom w decydowaniu o tym, które informacje udostępnią komu i w jaki sposób; zauważa, że w reakcji na doniesienia o masowej inwigilacji różne przedsiębiorstwa ogłosiły również plany umożliwienia pełnego szyfrowania (typu „end-to-end");

32. przypomina, że zgodnie z art. 15 ust. 1 dyrektywy 2000/31/WE państwa członkowskie nie mogą nakładać na usługodawców świadczących usługi transmisji, przechowywania i hostingu ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują, ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność; przypomina w szczególności, że Trybunał Sprawiedliwości Unii Europejskiej w wyrokach C-360/10 i C-70/10 odrzucił środki „aktywnego nadzoru" nad prawie wszystkimi usługobiorcami (w jednym wyroku chodziło o dostawców usług internetowych, a w drugim o sieć społecznościową) i sprecyzował, że wszelkie narzucanie podmiotom świadczącym usługi hostingu obowiązku prowadzenia ogólnego nadzoru jest zakazane;

33. z zadowoleniem przyjmuje publikowanie przez przedsiębiorstwa informatyczne i telekomunikacyjne sprawozdań poświęconych przejrzystości, które dotyczą wysuwanych przez rządy żądań dostępu do danych użytkowników; wzywa państwa członkowskie do publikowania statystyk uwzględniających liczbę ich żądań kierowanych do przedsiębiorstw prywatnych i dotyczących informacji o użytkownikach prywatnych;

Umowa w sprawie programu TFTP

34. jest rozczarowany tym, że Komisja zlekceważyła wyraźne wezwanie Parlamentu do zawieszenia umowy w sprawie programu TFTP ze względu na brak jasnych informacji doprecyzowujących, czy dane SWIFT byłyby pozyskiwane poza ramami umowy w sprawie TFTP przez jakikolwiek inny amerykański organ rządowy; zamierza uwzględnić ten fakt przy udzielaniu zgody na zawarcie międzynarodowych umów w przyszłości;

Wymiana innych danych osobowych z państwami trzecimi

35. podkreśla swoje stanowisko, że wszystkie umowy, mechanizmy i decyzje w sprawie odpowiedniej ochrony danych osobowych dotyczące wymiany z państwami trzecimi wiążącej się z danymi osobowymi wymagają ścisłego monitorowania i bezzwłocznych działań następczych ze strony Komisji jako strażniczki traktatów;

36. z zadowoleniem przyjmuje oświadczenie ryskie UE i USA z dnia 3 czerwca 2015 r. w sprawie zacieśniania współpracy transatlantyckiej w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, którego sygnatariusze zobowiązali się do sprawniejszego wdrażania Porozumienia między Unią Europejską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej (MLAT), zakończenia jego przeglądu zgodnie z porozumieniem i organizowania warsztatów w celu omawiania odnośnych kwestii z właściwymi organami krajowymi; podkreśla, że organy ścigania państw członkowskich powinny współpracować z organami państw trzecich w oparciu właśnie o porozumienia o wzajemnej pomocy prawnej (MLAT); w związku z tym wzywa państwa członkowskie i rząd USA do dotrzymania powyższych zobowiązań z myślą o szybkim zakończeniu przeglądu porozumienia MLAT między UE a USA;

37. wzywa Komisję do zdania sprawy Parlamentowi do końca 2015 r. z wykrytych w różnych instrumentach wykorzystywanych do międzynarodowych transferów danych luk dotyczących dostępu organów ścigania i służb wywiadowczych z państw trzecich do danych oraz do przedstawienia mu środków służących wyeliminowaniu tych luk, aby zapewnić ciągłość niezbędnej właściwej ochrony danych osobowych przesyłanych z UE do państw trzecich;

Ochrona praworządności i praw podstawowych obywateli UE/zwiększona ochrona osób zgłaszających przypadki naruszenia oraz dziennikarzy

38. uważa, że prawa podstawowe obywateli UE pozostają zagrożone i że zbyt mało zrobiono, by zapewnić ich pełną ochronę w razie masowej inwigilacji elektronicznej; ubolewa nad niewielkimi postępami w zapewnianiu ochrony osobom zgłaszającym przypadki naruszenia i dziennikarzom;

39. ubolewa nad faktem, że wiele programów wywiadowczych na masową i szeroką skalę jest najwyraźniej kierowanych również interesami ekonomicznymi przedsiębiorstw, które opracowują i realizują te programy, co miało miejsce w przypadku zakończenia ukierunkowanego programu NSA „Thinthread" i zastąpienia go programem inwigilacji na dużą skalę „Trailblazer", który zlecono SAIC w 2001 r.;

40. ponownie zgłasza poważne obawy związane z pracami komisji Rady Europy ds. Konwencji o cyberprzestępczości w zakresie interpretacji art. 32 Konwencji o cyberprzestępczości z dnia 23 listopada 2001 r. (konwencja budapeszteńska) w odniesieniu do transgranicznego dostępu do danych przechowywanych w formie elektronicznej za zgodą lub w przypadku ich powszechnej dostępności i sprzeciwia się podpisywaniu protokołu dodatkowego lub wytycznych, mających na celu poszerzenie zakresu tego postanowienia, tak aby wykraczało poza obowiązujący system wprowadzony na mocy tej konwencji, który już w obecnej formie stanowi znaczący wyjątek od zasady terytorialności, ponieważ mogłoby to skutkować nieskrępowanym zdalnym dostępem organów ścigania do serwerów i komputerów zlokalizowanych w innych jurysdykcjach bez zastosowania porozumień w sprawie wzajemnej pomocy prawnej i innych instrumentów współpracy sądowej wprowadzonych w celu zagwarantowania praw podstawowych jednostki, w tym ochrony danych i rzetelnego procesu; podkreśla, że Unia Europejska wykonuje swoje uprawnienia w zakresie cyberprzestępczości i dlatego należy przestrzegać prerogatyw zarówno Komisji, jak i Parlamentu;

41. ubolewa nad tym, że Komisja nie odpowiedziała na wniosek Parlamentu, by przeprowadziła ona analizę dotyczącą kompleksowego europejskiego programu ochrony osób zgłaszających przypadki naruszenia, oraz wzywa Komisję do przedstawienia najpóźniej do końca 2016 r. komunikatu na ten temat;

42. z zadowoleniem przyjmuje rezolucję przyjętą w dniu 23 czerwca 2015 r. przez Zgromadzenie Parlamentarne Rady Europy w sprawie zwiększenia ochrony osób zgłaszających przypadki naruszenia, zwłaszcza jej ust. 9 dotyczący znaczenia, jakie zgłaszanie przypadków naruszenia ma dla przestrzegania ograniczeń prawnych w dziedzinie inwigilacji, oraz jej ust. 10, w którym wezwano UE do uchwalenia przepisów o ochronie osób zgłaszających przypadki naruszenia, które obejmowałyby również pracowników krajowych służb bezpieczeństwa i wywiadu oraz przedsiębiorstw prywatnych działających w tej branży, a także do udzielania azylu, w miarę możliwości na mocy prawa krajowego, osobom zgłaszającym przypadki naruszenia, którym grozi odwet w ich kraju pochodzenia, pod warunkiem że osoby te kwalifikują się ze względu na charakter ujawnionych przez nie informacji do objęcia ochroną w oparciu o zasady popierane przez to Zgromadzenie;

43. podkreśla, że masowa inwigilacja rażąco podważa zasadę tajemnicy zawodowej zawodów regulowanych, w tym lekarzy, dziennikarzy i prawników; zwraca w szczególności uwagę na prawo obywateli UE do ochrony poufnej wymiany informacji z ich adwokatami przed wszelką inwigilacją, która naruszałaby postanowienia Karty praw podstawowych Unii Europejskiej, w szczególności jej art. 6, 47 i 48, oraz przepisy dyrektywy 2013/48/UE w sprawie prawa dostępu do adwokata; wzywa Komisję do przedstawienia najpóźniej do końca 2016 r. komunikatu w sprawie ochrony poufnej wymiany informacji w zawodach, w przypadku których wymagana jest poufność wymiany informacji między prawnikiem a klientem;

44. wzywa Komisję do przygotowania wytycznych dla państw członkowskich na temat tego, jak dostosować wszelkie instrumenty gromadzenia danych osobowych do celów zapobiegania przestępstwom, prowadzenia dochodzeń, wykrywania i ścigania przestępstw, w tym terroryzmu, do wyroków Trybunału Sprawiedliwości UE z dnia 8 kwietnia 2014 r. w sprawie zatrzymywania danych (sprawy C-293/12 i C-594/12) oraz z dnia 6 października 2015 r. w sprawie bezpiecznego transferu danych osobowych (sprawa C-362/14); zwraca szczególną uwagę na ust. 58 i 59 wyroku w sprawie zatrzymywania danych oraz na ust. 93 i 94 wyroku w sprawie bezpiecznego transferu danych osobowych, które jasno wymagają ukierunkowanego podejścia do gromadzenia danych zamiast zatrzymywania wszystkich danych;

45. zwraca uwagę na fakt, że najnowsze orzecznictwo, w szczególności wyrok TFUE z dnia 8 kwietnia 2014 r. w sprawie zatrzymywania danych, ustanawia wyraźny wymóg prawny polegający na wykazaniu konieczności i proporcjonalności wszelkich środków obejmujących gromadzenie i wykorzystywanie danych osobowych, które to środki mogą potencjalnie kolidować z prawem do ochrony życia prywatnego i rodzinnego oraz prawem ochrony danych; ubolewa nad tym, że względy polityczne często negatywnie wpływają na przestrzeganie tych zasad prawnych w procesie podejmowania decyzji; wzywa Komisję do zapewnienia w ramach Programu lepszego stanowienia prawa, by całe prawo UE cechowało się wysoką jakością, spełniało wszystkie normy prawne i było zgodne z orzecznictwem, a także z postanowieniami Karty praw podstawowych Unii Europejskiej; zaleca każdorazowe uwzględnianie testu konieczności i proporcjonalności w ocenie skutków wszystkich środków egzekwowania prawa i zapewniania bezpieczeństwa obejmujących zastosowanie i gromadzenie danych osobowych;

Europejska strategia na rzecz większej niezależności w dziedzinie IT

46. jest rozczarowany brakiem działania ze strony Komisji w celu zastosowania się do wydanych w rezolucji szczegółowych zaleceń dotyczących zwiększenia bezpieczeństwa informatycznego i ochrony prywatności w internecie na szczeblu UE;

47. z zadowoleniem przyjmuje kroki poczynione dotychczas w celu zwiększenia bezpieczeństwa informatycznego Parlamentu, o czym mowa w planie działania DG ITEC dotyczącym bezpieczeństwa ICT Parlamentu Europejskiego; domaga się, by starania te były kontynuowane oraz by wydane w rezolucji zalecenia zostały w pełni i szybko wdrożone; apeluje o nowe spojrzenie, a w razie potrzeby o zmiany ustawodawcze w zakresie udzielania zamówień publicznych, aby zwiększyć bezpieczeństwo informatyczne instytucji UE; apeluje o systematyczne zastępowanie we wszystkich instytucjach UE oprogramowania zamkniętego oprogramowaniem otwartym, które można poddać kontroli i weryfikacji, oraz o wprowadzenie obowiązkowego kryterium „otwartości" we wszystkich przyszłych procedurach udzielania zamówień w dziedzinie ICT, jak też o faktyczną dostępność narzędzi szyfrujących;

48. stanowczo ponawia wezwanie do opracowania – w ramach nowych inicjatyw takich jak jednolity rynek cyfrowy – europejskiej strategii na rzecz większej niezależności w dziedzinie IT i ochrony prywatności w internecie, która stanie się bodźcem dla przemysłu informatycznego w UE;

49. zamierza przedstawić dalsze zalecenia w tej dziedzinie po zaplanowanej przez Parlament na koniec 2015 r. konferencji na temat ochrony życia prywatnego w internecie dzięki zwiększeniu bezpieczeństwa informatycznego i autonomii informatycznej UE, z wykorzystaniem ustaleń z niedawnego badania panelu STOA na temat masowej inwigilacji użytkowników IT;

Demokratyczne i neutralne zarządzanie internetem

50. z zadowoleniem przyjmuje cel Komisji, jakim jest uczynienie z UE podmiotu referencyjnego, jeśli chodzi o zarządzanie internetem, oraz jej wizję wielostronnego modelu zarządzania internetem potwierdzoną na Globalnym wielostronnym posiedzeniu w sprawie przyszłości zarządzania internetem (NETMundial) w kwietniu 2014 r. w Brazylii; oczekuje rezultatów trwających obecnie międzynarodowych prac w tej dziedzinie, w tym w ramach Forum Zarządzania Internetem;

51. przestrzega przed oczywistą negatywną spiralą dotyczącą przestrzegania prawa podstawowego do prywatności i ochrony danych osobowych, która następuje, kiedy każdą informację o czyimś zachowaniu uznaje się za potencjalnie istotną z punktu widzenia przyszłej walki z przestępczością, co musi powodować masową inwigilację, w której każdy obywatel jest traktowany jak potencjalny podejrzany, i prowadzić do zaniku spójności społecznej i zaufania społecznego;

52. zamierza uwzględnić ustalenia Agencji Praw Podstawowych zawarte w szczegółowym badaniu na temat ochrony praw podstawowych w kontekście inwigilacji, zwłaszcza dotyczące aktualnej sytuacji prawnej obywateli ze względu na środki odwoławcze, jakie im przysługują w związku z tymi praktykami;

Działania następcze

53. zobowiązuje swoją Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych do dalszego monitorowania postępów w tej dziedzinie oraz do śledzenia, czy realizowane są zalecenia sformułowane w rezolucji;

o

o o

54. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji, a także rządom i parlamentom państw członkowskich oraz Radzie Europy.