Środa, 12 marca 2014 r.

P7_TA(2014)0230

Realizowane przez NSA amerykańskie programy nadzoru, organy nadzoru w różnych państwach członkowskich oraz wpływ na prawa podstawowe obywateli UE

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))

(2017/C 378/14)

Parlament Europejski,

— uwzględniając Traktat o Unii Europejskiej (TUE), w szczególności jego art. 2, 3, 4, 5, 6, 7, 10, 11 i 21,

— uwzględniając Traktat o funkcjonowaniu Unii Europejskiej (TFUE), w szczególności jego art. 15, 16 i 218 oraz tytuł V,

— uwzględniając protokół nr 36 w sprawie postanowień przejściowych oraz jego art. 10, a także deklarację nr 50 dotyczącą tego protokołu,

— uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 i 52,

— uwzględniając europejską konwencję praw człowieka, w szczególności jej art. 6, 8, 9, 10 i 13 oraz protokoły do tej konwencji,

— uwzględniając Powszechną deklarację praw człowieka, szczególnie jej art. 7, 8, 10, 11, 12 i 14 ([1]),

— uwzględniając Międzynarodowy pakt praw obywatelskich i politycznych, zwłaszcza jego art. 14, 17, 18 i 19,

— uwzględniając konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108) oraz protokół dodatkowy do tej konwencji z dnia 8 listopada 2001 r.dotyczący organów nadzoru oraz transgranicznego przepływu danych (ETS nr 181),

— uwzględniając Konwencję wiedeńską o stosunkach dyplomatycznych, zwłaszcza jej art. 24, 27 i 40,

— uwzględniając Konwencję Rady Europy o cyberprzestępczości (ETS nr 185),

— uwzględniając sprawozdanie specjalnego sprawozdawcy ONZ w sprawie propagowania i ochrony praw człowieka i wolności podstawowych w warunkach walki z terroryzmem, przedłożone dnia 17 maja 2010 r. ([2]),

— uwzględniając komunikat Komisji zatytułowany „Polityka wobec internetu i zarządzanie internetem –rola Europy w kształtowaniu przyszłości zarządzania internetem" (COM(2014)0072);

— uwzględniając sprawozdanie specjalnego sprawozdawcy ONZ w sprawie propagowania i ochrony prawa wolności opinii i wypowiedzi, przedłożone dnia 17 kwietnia 2013 r. ([3]),

— uwzględniając wytyczne w sprawie praw człowieka oraz zwalczania terroryzmu przyjęte przez Komitet Ministrów Rady Europy dnia 11 lipca 2002 r.,

([1]) http://www.unic.un.org.pl/prawa_czlowieka/dok_powszechna_deklaracja.php
([2]) http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement
([3]) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

— uwzględniając deklarację brukselską przyjętą w dniu 1 października 2010 r. podczas szóstej konferencji komisji parlamentarnych właściwych ds. nadzoru nad służbami wywiadowczymi i bezpieczeństwa państw członkowskich Unii Europejskiej,

— uwzględniając uchwałę Zgromadzenia Parlamentarnego Rady Europy nr 1954 (2013) w sprawie bezpieczeństwa narodowego i dostępu do informacji,

— uwzględniając sprawozdanie w sprawie demokratycznego nadzoru nad służbami bezpieczeństwa przyjęte przez Komisję Wenecką dnia 11 czerwca 2007 r. ([1]) oraz oczekując z dużym zainteresowaniem na jego aktualizację zapowiedzianą na wiosnę 2014 r.,

— uwzględniając zeznania przedstawicieli komisji nadzoru służb wywiadowczych z Belgii, Niderlandów, Danii i Norwegii,

— uwzględniając sprawy wniesione do sądów francuskich ([2]), polskich i brytyjskich ([3]), jak również Europejskiego Trybunału Praw Człowieka ([4]), w związku z systemami nadzoru prowadzonego na masową skalę,

— uwzględniając ustanowioną przez Radę zgodnie z art. 34 Traktatu o Unii Europejskiej Europejską konwencję o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej ([5]), w szczególności jej tytuł III,

— uwzględniając decyzję Komisji 2000/520/WE z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady bezpiecznego transferu danych osobowych oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA,

— uwzględniając sprawozdania oceniające Komisji w sprawie wdrożenia zasad bezpiecznego transferu danych osobowych z dnia 13 lutego 2002 r. (SEC(2002)0196) oraz z dnia 20 października 2004 r. (SEC(2004)1323),

— uwzględniając komunikat Komisji z dnia 27 listopada 2013 r. w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE (COM(2013)0847) oraz komunikat Komisji z dnia 27 listopada 2013 r. w sprawie odbudowy zaufania do przypływów danych między Unią Europejską a Stanami Zjednoczonymi (COM(2013)0846),

— uwzględniając rezolucję Parlamentu Europejskiego z dnia 5 lipca 2000 r. w sprawie projektu decyzji Komisji w sprawie adekwatności ochrony przewidzianej przez zasady bezpiecznego transferu danych osobowych oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA ([6]), z której wynika, że nie można potwierdzić adekwatności systemu, a także uwzględniając opinie Grupy Roboczej Art. 29, w szczególności opinię 4/2000 z dnia 16 maja 2000 r. ([7]),

— uwzględniając umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych (umowa w sprawie PNR) z 2004 r., 2007 r. ([8]) i 2012 r. ([9]),

— uwzględniając wspólny przegląd realizacji Umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o przetwarzaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych ([10]), towarzyszący sprawozdaniu Komisji dla Parlamentu Europejskiego i Rady w sprawie wspólnego przeglądu (COM(2013)0844),

---

([1]) http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
([2]) La Fédération Internationale des Ligues des Droits de l'Homme i La Ligue française pour la défense des droits de l'Homme et du Citoyen v. X; Tribunal de Grande Instance of Paris.
([3]) Sprawy wniesione przez Privacy International and Liberty do Investigatory Powers Tribunal.
([4]) Wspólny pozew złożony na mocy art. 34 przez Big Brother Watch, Open Rights Group, English PEN i Dr Constanze Kurz (skarżący) v. United Kingdom (pozwany).
([5]) Dz.U. C 197 z 12.7.2000, s. 1.
([6]) Dz.U. C 121 z 24.4.2001, s. 152.
([7]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
([8]) Dz.U. L 204 z 4.8.2007, s. 18.
([9]) Dz.U. L 215 z 11.8.2012, s. 5.
([10]) SEC(2013)0630, 27.11.2013.

— uwzględniając opinię rzecznika generalnego Cruza Villalóna, z której wynika, że dyrektywa 2006/24/WE w sprawie zatrzymania danych generowanych lub przetwarzanych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności jest w całości niezgodna z art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej oraz że art. 6 tej dyrektywy jest niezgodny z art. 7 i art. 52 ust. 1 karty ([1]),

— uwzględniając decyzję Rady 2010/412/UE z dnia 13 lipca 2010 r. w sprawie zawarcia Umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu z Unii Europejskiej do Stanów Zjednoczonych danych z komunikatów finansowych do celów Programu śledzenia środków finansowych należących do terrorystów (TFTP) ([2]) oraz załączone do niej oświadczenia Komisji i Rady,

— uwzględniając Porozumienie między Unią Europejską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej ([3]),

— uwzględniając trwające negocjacje dotyczące umowy ramowej między Unią Europejską a Stanami Zjednoczonymi w sprawie ochrony danych osobowych przekazywanych i przetwarzanych do celów działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych, w tym terroryzmu, w ramach współpracy policyjnej i sądowej w sprawach karnych (tzw. umowy parasolowej),

— uwzględniając rozporządzenie Rady (WE) nr 2271/96 z dnia 22 listopada 1996 r. zabezpieczające przed skutkami eksterytorialnego stosowania ustawodawstwa przyjętego przez państwo trzecie oraz działaniami opartymi na nim lub z niego wynikającymi ([4]),

— uwzględniając oświadczenie prezydenta Federacyjnej Republiki Brazylii złożone podczas otwarcia 68. sesji Zgromadzenia Ogólnego ONZ dnia 24 września 2013 r. oraz prace prowadzone przez parlamentarną komisję śledczą ds. szpiegostwa powołaną przez Federalny Senat Brazylii,

— uwzględniając amerykańską ustawę PATRIOT podpisaną przez prezydenta George'a W. Busha dnia 26 października 2001 r.,

— uwzględniając amerykańską ustawę o nadzorze zagranicznego wywiadu (FISA) z 1978 r. oraz ustawę zmieniającą z 2008 r.,

— uwzględniając zarządzenie wykonawcze nr 12333 wydane przez prezydenta Stanów Zjednoczonych w 1981 r. wraz ze zmianami z 2008 r.,

— uwzględniając rozporządzenie prezydenta (PPD-28) w sprawie działań wywiadu sygnałów wydane przez prezydenta Stanów Zjednoczonych Baracka Obamę w dniu 17 stycznia 2014 r.,

— uwzględniając wnioski ustawodawcze rozpatrywane obecnie przez Kongres Stanów Zjednoczonych, w tym projekt amerykańskiej ustawy o wolności (Freedom Act), projekt ustawy o reformie kontroli i nadzoru nad służbami wywiadowczymi i inne,

— uwzględniając przeglądy przeprowadzone przez Radę ds. Nadzoru Prywatności i Wolności Obywatelskich, amerykańską Radę Bezpieczeństwa Narodowego oraz prezydencką grupę oceniającą ds. wywiadu i technologii komunikacyjnej, w szczególności sprawozdanie tej ostatniej z dnia 12 grudnia 2013 r. zatytułowane „Liberty and Security in a Changing World" [Wolność i bezpieczeństwo w zmieniającym się świecie],

— uwzględniając orzeczenie amerykańskiego sądu okręgowego dla Dystryktu Kolumbia w sprawie Klayman i in. przeciwko Obamie i in., powództwo cywilne nr 13-0851 z dnia 16 grudnia 2013 r. oraz orzeczenie amerykańskiego sądu okręgowego dla Dystryktu Nowy Jork-Południe w sprawie ACLU i in. przeciwko Jamesowi R. Clapperowi i in., powództwo cywilne nr 13-3994 z dnia 11 czerwca 2013 r.,

— uwzględniając sprawozdanie w sprawie ustaleń unijnych współprzewodniczących tymczasowej grupy roboczej UE-USA ds. ochrony danych z dnia 27 listopada 2013 r. ([5]),

---

([1]) Opinia rzecznika generalnego Cruza Villalóna z dnia 12 grudnia 2013 r. w sprawie C-293/12.
([2]) Dz.U. L 195 z 27.7.2010, s. 3.
([3]) Dz.U. L 181 z 19.7.2003, s. 34.
([4]) Dz.U. L 309 z 29.11.1996, s. 1.
([5]) Dokument Rady 16987/2013.

— uwzględniając swą rezolucję z dnia 5 września 2001 r. ([1]) oraz dnia 7 listopada 2002 r. ([2]) w sprawie istnienia ogólnoświatowego systemu przechwytywania komunikacji prywatnej i handlowej (systemu podsłuchu ECHELON),

— uwzględniając swą rezolucję z dnia 21 maja 2013 r. w sprawie Karty praw podstawowych UE: standardy określające wolność mediów w UE ([3]),

— uwzględniając swą rezolucję z dnia 4 lipca 2013 r. w sprawie programu inwigilacji amerykańskiej Agencji Bezpieczeństwa Narodowego, służb wywiadowczych w różnych państwach członkowskich i wpływu na prywatność obywateli UE ([4]), w której zaleca Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych przeprowadzenie szczegółowego dochodzenia w tej sprawie,

— uwzględniając dokument roboczy nr 1 w sprawie amerykańskich i unijnych programów nadzoru oraz ich wpływu na prawa podstawowe obywateli UE,

— uwzględniając dokument roboczy nr 3 w sprawie zależności między praktykami nadzoru w UE i USA a unijnymi przepisami dotyczącymi ochrony danych osobowych,

— uwzględniając dokument roboczy nr 4 w sprawie amerykańskich działań w zakresie nadzoru w odniesieniu do danych unijnych oraz możliwych implikacji prawnych takich działań dla umów transatlantyckich i współpracy transatlantyckiej,

— uwzględniając dokument roboczy nr 5 w sprawie demokratycznej kontroli służb wywiadowczych państw członkowskich i organów wywiadowczych UE,

— uwzględniając dokument roboczy Komisji Spraw Zagranicznych w sprawie aspektów polityki zagranicznej w związku z dochodzeniem w sprawie masowego nadzoru elektronicznego obywateli UE;

— uwzględniając swą rezolucję z dnia 23 października 2013 r. w sprawie przestępczości zorganizowanej, korupcji i prania pieniędzy: zalecenia dotyczące potrzebnych działań i inicjatyw ([5]),

— uwzględniając swą rezolucję z dnia 23 października 2013 r. w sprawie zawieszenia umowy TFTP w następstwie inwigilacji prowadzonej przez Agencje Bezpieczeństwa Narodowego USA ([6]),

— uwzględniając swą rezolucję z dnia 10 grudnia 2013 r. w sprawie wykorzystania potencjału chmury obliczeniowej w Europie ([7]),

— uwzględniając porozumienie międzyinstytucjonalne między Parlamentem Europejskim a Radą w sprawie przekazywania Parlamentowi Europejskiemu i wykorzystywania przez Parlament Europejski posiadanych przez Radę informacji niejawnych dotyczących spraw innych niż z dziedziny wspólnej polityki zagranicznej i bezpieczeństwa ([8]),

— uwzględniając załącznik VIII do Regulaminu,

— uwzględniając art.48 Regulaminu,

— uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (A7-0139/2014),

Wpływ masowej inwigilacji

A. mając na uwadze, że ochrona danych i prywatności to prawa podstawowe; mając na uwadze, że środki bezpieczeństwa, w tym środki na rzecz zwalczania terroryzmu, muszą być zatem realizowane w ramach rządów prawa i muszą podlegać wymogom w zakresie praw podstawowych, w tym wymogom odnoszącym się do ochrony prywatności i ochrony danych;

([1]) Dz.U. C 72 E z 21.3.2002, s. 221.
([2]) Dz.U. C 16 E z 22.1.2004, s. 88.
([3]) Teksty przyjęte, P7_TA(2013)0203.
([4]) Teksty przyjęte, P7_TA(2013)0322.
([5]) Teksty przyjęte, P7_TA(2013)0444.
([6]) Teksty przyjęte, P7_TA(2013)0449.
([7]) Teksty przyjęte, P7_TA(2013)0535.
([8]) Dz.U. C 353 E z 3.12.2013, s. 156.

B. mając na uwadze, że przepływ informacji i danych, dominujący obecnie w życiu codziennym i będący częścią integralności każdej jednostki, musi być tak zabezpieczony przed ingerencją jak prywatne domy;

C. mając na uwadze, że związki między Europą a Stanami Zjednoczonymi Ameryki opierają się na duchu i zasadach demokracji oraz na praworządności, wolności, sprawiedliwości i solidarności;

D. mając na uwadze, że współpraca w zakresie zwalczania terroryzmu między Stanami Zjednoczonymi a Unią Europejską i jej państwami członkowskimi ma nadal istotne znaczenie dla bezpieczeństwa obu stron;

E. mając na uwadze, że wzajemne zaufanie i zrozumienie to kluczowe elementy dialogu i partnerstwa transatlantyckiego;

F. mając na uwadze, że w następstwie wydarzeń z 11 września 2001 r., walka z terroryzmem stała się jednym z głównych priorytetów większości rządów; mając na uwadze, że doniesienia oparte na dokumentach ujawnionych przez byłego pracownika amerykańskiej Agencji Bezpieczeństwa Krajowego (NSA) Edwarda Snowdena zmusiły przywódców politycznych do zmierzenia się z wyzwaniem, jakim jest kontrola i nadzór agencji wywiadu w zakresie działań inwigilacyjnych, a także ocena wpływu prowadzonych przez nie działań na prawa podstawowe oraz praworządność w społeczeństwie demokratycznym;

G. mając na uwadze, że od czerwca 2013 r. wspomniane doniesienia wywołały w UE liczne obawy dotyczące:

— zakresu systemów nadzoru ujawnionego zarówno przez Stany Zjednoczone, jak i państwa członkowskie UE;

— naruszenia unijnych norm prawnych, praw podstawowych oraz norm ochrony danych osobowych;

— poziomu zaufania między UE a USA jako partnerami transatlantyckimi;

— stopnia współpracy i zaangażowania niektórych państw członkowskich UE w amerykańskie programy nadzoru lub analogicznych programów realizowanych na szczeblu krajowym, co ujawniły media;

— braku kontroli i skutecznego nadzoru ze strony amerykańskich władz politycznych i niektórych państw członkowskich UE nad ich środowiskami wywiadowczymi;

— możliwości wykorzystywania masowej inwigilacji w celach niezwiązanych z bezpieczeństwem narodowymi i bezpośrednią walką z terroryzmem, np. szpiegostwo gospodarcze i przemysłowe lub profilowanie pod względem przekonań politycznych;

— podważania wolności pracy i komunikacji przedstawicieli zawodów, których obowiązuje tajemnica zawodowa, w tym prawników i lekarzy;

— odnośnych ról oraz stopnia zaangażowania agencji wywiadu oraz prywatnych spółek informatycznych i telekomunikacyjnych;

— coraz bardziej zacierających się granic między egzekwowaniem prawa a działaniami wywiadowczymi, co prowadzi do traktowania każdego obywatela jako osoby podejrzanej i obejmowania go nadzorem;

— zagrożenia prywatności w erze cyfrowej i oddziaływanie masowego nadzoru na obywateli i społeczeństwa;

H. mając na uwadze, że bezprecedensowa skala ujawnionego szpiegostwa wymaga dogłębnego śledztwa ze strony władz amerykańskich, instytucji europejskich oraz rządów, parlamentów narodowych i organów wymiaru sprawiedliwości państw członkowskich;

I. mając na uwadze, że władze amerykańskie zdementowały część ujawnionych informacji, ale nie zaprzeczyły większości z nich; mając na uwadze szeroko zakrojoną debatę publiczną, która wywiązała się w Stanach Zjednoczonych i w niektórych państwach członkowskich UE; mając na uwadze, że rządy i parlamenty państw UE zbyt często zachowują milczenie i nie wszczynają odpowiednich dochodzeń;

J. mając na uwadze, że prezydent Obama zapowiedział niedawno reformę NSA oraz jej programów nadzoru;

K. mając na uwadze, że w przeciwieństwie do obydwu instytucji UE oraz niektórych państw członkowskich Parlament Europejski bardzo poważnie potraktował obowiązek wyjaśnienia doniesień dotyczących prowadzonego na masową skalę bezkrytycznego nadzoru obywateli UE i w swej rezolucji z dnia 4 lipca 2013 r. w sprawie programu inwigilacji amerykańskiej Agencji Bezpieczeństwa Narodowego, służb wywiadowczych w różnych państwach członkowskich i ich wpływu na obywateli UE poinstruował Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, aby przeprowadziła gruntowne dochodzenie w tej sprawie;

L. mając na uwadze, że obowiązkiem instytucji europejskich jest dopilnowanie, aby prawo unijne było wdrażane w pełni, z korzyścią dla obywateli UE, a także aby nie podważano mocy prawnej traktatów UE za sprawą lekceważącej akceptacji eksterytorialnych skutków norm lub działań państw trzecich;

Postępy Stanów Zjednoczonych w reformowaniu wywiadu

M. mając na uwadze, że Sąd Okręgowy dla Dystryktu Kolumbia w orzeczeniu z dnia 16 grudnia 2013 r. uznał, że masowe gromadzenie metadanych przez NSA stanowi naruszenie czwartej poprawki do konstytucji amerykańskiej ([1]); mając przy tym na uwadze, że Sąd Okręgowy dla Dystryktu Nowy Jork-Południe w orzeczeniu z dnia 27 grudnia 2013 r. stwierdził zgodność z prawem takiego gromadzenia danych;

N. mając, na uwadze, że Sąd Okręgowy dla Wschodniego Dystryktu Michigan orzekł, że czwarta poprawka wymaga zasadności wszystkich przeszukań, dysponowania nakazem przed przystąpieniem do uzasadnionego przeszukania, wydawania nakazów w oparciu o wcześniejsze zaistnienie uzasadnionych podstaw ich wydania, a także konkretnego odniesienia do osoby, miejsca i rzeczy, jak również interwencji neutralnego urzędnika stojącego między funkcjonariuszami egzekwowania prawa władzy wykonawczej a obywatelami ([2]);

O. mając na uwadze, że w sprawozdaniu z dnia 12 grudnia 2013 r. prezydenckiej grupy oceniającej ds. wywiadu i technologii komunikacyjnej przedstawiono prezydentowi Stanów Zjednoczonych propozycje 46 zaleceń; mając na uwadze, że w zaleceniach podkreślono potrzebę jednoczesnego zapewnienia ochrony bezpieczeństwa narodowego oraz prywatności i wolności obywatelskich; mając na uwadze, że w związku z powyższym zachęca się rząd USA do jak najszybszego zaprzestania masowego gromadzenia rejestrów połączeń telefonicznych osób ze Stanów Zjednoczonych zgodnie z art. 215 ustawy Patriot Act, do przeprowadzenia szczegółowego przeglądu ram prawnych dotyczących NSA i wywiadu amerykańskiego w celu zapewnienia poszanowania prawa do prywatności, do zaprzestania działań mających na celu obchodzenie lub narażenie oprogramowania komercyjnego (poprzez lukę w zabezpieczeniach lub złośliwe oprogramowanie), do szerszego stosowania szyfrowania, szczególnie w przypadku danych podlegających transferom, a także do zaniechania umniejszania znaczenia działań służących stworzeniu standardów szyfrowania, do powołania rzecznika interesu publicznego, który stałby w obronie prywatności oraz wolności obywatelskich przed Sądem ds. Nadzoru Zagranicznego Wywiadu, do nadania Radzie ds. Prywatności i Wolności Obywatelskich uprawnień w zakresie nadzoru nad działaniami Wspólnoty Wywiadów w celach związanych z wywiadem zagranicznym, a nie tylko zwalczaniem terroryzmu, a także do przyjmowania skarg osób zgłaszających przypadki naruszenia, stosowania układów o wzajemnej pomocy prawnej w celu uzyskania komunikacji elektronicznej oraz do niewykorzystywania nadzoru do kradzieży tajemnic przedsiębiorstw i tajemnic handlowych;

P. mając na uwadze, że zgodnie z pismem otwartym przekazanym prezydentowi Obamie przez byłych członków kadry kierowniczej NSA/członków grupy Veteran Intelligence Professionals for Sanity (VIPS) z dnia 7 stycznia 2014 r. ([3]) masowe gromadzenie danych nie gwarantuje większych możliwości przewidywania przyszłych ataków terrorystycznych; mając na uwadze, że autorzy pisma podkreślają, iż nadzór prowadzony na masową skalę przez NSA nie zapobiegł żadnemu atakowi, przy czym wydano miliardy dolarów na programy, które są mniej efektywne i w dużo większym stopniu ingerują w prywatność obywateli niż technologia wewnętrzna, znana jako THINTHREAD, opracowana w 2001 r.;

Q. mając na uwadze, że w kwestii działań wywiadowczych dotyczących osób spoza Stanów Zjednoczonych zgodnie z art. 702 ustawy FISA zalecenia przedstawione prezydentowi Stanów Zjednoczonych obejmują fundamentalną kwestię poszanowania prywatności oraz godności ludzkiej zapisaną w art. 12 Powszechnej deklaracji praw człowieka oraz art. 17 Międzynarodowego paktu praw obywatelskich i politycznych; mając na uwadze, że nie obejmują one przyznania osobom spoza Stanów Zjednoczonych takich samych praw i takiej samej ochrony, jakie przysługują osobom ze Stanów Zjednoczonych;

([1]) Klayman i in. przeciwko Obamie i in., powództwo cywilne nr 13-0851, 16 grudnia 2013 r.
([2]) ACLU przeciwko NSA nr 06-CV-10204, 17 sierpnia 2006 r.
([3]) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

R. mając na uwadze, że prezydent Stanów Zjednoczonych Barack Obama w rozporządzeniu z dnia 17 stycznia 2014 r. w sprawie działań wywiadu sygnałów oraz przemówieniu na ten temat stwierdził, że prowadzony na masową skalę nadzór elektroniczny jest konieczny, aby Stany Zjednoczone mogły chronić swoje bezpieczeństwo narodowe, swych obywateli oraz obywateli amerykańskich sojuszników i partnerów, jak również aby mogły czynić postępy w zakresie polityki zagranicznej; mając na uwadze, że rozporządzenie to zawiera szereg zasad dotyczących gromadzenia, wykorzystywania i wymiany informacji uzyskanych przez wywiad sygnałów oraz obejmuje niektórymi zabezpieczeniami osoby spoza USA, częściowo przewidując traktowanie równorzędne z traktowaniem obywateli Stanów Zjednoczonych, w tym zabezpieczanie danych osobowych wszystkich osób, niezależnie od ich obywatelstwa lub miejsca zamieszkania; mając na uwadze, że prezydent Obama nie domagał się żadnych konkretnych propozycji, dotyczących szczególnie zakazu prowadzenia nadzoru na masową skalę oraz wprowadzenia środków administracyjnych i sądowych umożliwiających dochodzenie roszczeń osobom spoza Stanów Zjednoczonych;

Ramy prawne

Prawa podstawowe

S. mając na uwadze, że sprawozdanie w sprawie ustaleń unijnych współprzewodniczących tymczasowej grupy roboczej UE-USA ds. ochrony danych zawiera opis sytuacji prawnej w Stanach Zjednoczonych, ale nie przedstawia faktów dotyczących amerykańskich programów nadzoru; mając na uwadze, że nie udostępniono żadnych informacji na temat tzw. grupy roboczej „drugiej ścieżki", w ramach której państwa członkowskie dwustronnie omawiają z władzami amerykańskimi kwestie związane z bezpieczeństwem narodowym;

T. mając na uwadze, że prawa podstawowe, szczególnie wolność wypowiedzi, prasy, myśli, sumienia, wyznania oraz wolność zrzeszania się, prawo do prywatności, ochrona danych osobowych, a także prawo do skutecznego środka odwoławczego, domniemanie niewinności oraz prawo do rzetelnego procesu sądowego i brak dyskryminacji, zapisane w Karcie praw podstawowych Unii Europejskiej oraz europejskiej konwencji praw człowieka, stanowią podwaliny demokracji; mając na uwadze, że prowadzenie na masową skalę nadzoru nad ludźmi nie jest spójne z tymi fundamentami;

U. mając na uwadze, że we wszystkich państwach członkowskich prawo chroni przed ujawnianiem poufnych informacji powierzonych prawnikowi przez klienta, którą to zasadę uznaje Trybunał Sprawiedliwości Unii Europejskiej ([1]);

V. mając na uwadze, że w swej rezolucji z dnia 23 października 2013 r. w sprawie przestępczości zorganizowanej, korupcji oraz prania pieniędzy Parlament wezwał Komisję do przedstawienia wniosku ustawodawczego wprowadzającego skuteczny i kompleksowy europejski program ochrony osób zgłaszających przypadki naruszenia w celu ochrony interesów finansowych UE, a także do przeprowadzania analizy, czy takie ustawodawstwo powinno w przyszłości obejmować również inne dziedziny wchodzące w zakres uprawnień Unii;

Kompetencje Unii w dziedzinie bezpieczeństwa

W. mając na uwadze, że zgodnie z art. 67 ust. 3 TFUE Unia Europejska „dokłada starań, aby zapewnić wysoki poziom bezpieczeństwa"; mając na uwadze, że postanowienia Traktatu (szczególnie art. 4 ust. 2 TUE, art. 72 TFUE i art. 73 TFUE) skutkują tym, iż UE posiada pewne uprawnienia w kwestiach związanych ze zbiorowym bezpieczeństwem Unii; mając na uwadze, że UE posiada uprawnienia w kwestiach bezpieczeństwa wewnętrznego (art. 4 lit. j) TFUE) i realizuje te uprawnienia, decydując o szeregu instrumentów ustawodawczych oraz zawierając umowy międzynarodowe (PNR, TFTP) mające na celu zwalczanie poważnej przestępczości i terroryzmu, a także określając strategię w zakresie bezpieczeństwa wewnętrznego i powołując agencje działające w tej dziedzinie;

X. mając na uwadze, że Traktat o funkcjonowaniu Unii Europejskiej stanowi, iż „Państwa Członkowskie mogą organizować między sobą i na swoją odpowiedzialność uznane przez nie za stosowne formy współpracy i koordynacji między właściwymi służbami ich administracji odpowiedzialnymi za zapewnienie bezpieczeństwa narodowego" (art. 73 TFUE);

Y. mając na uwadze, że art. 276 TFUE stanowi, iż „W wykonywaniu swoich uprawnień dotyczących postanowień części trzeciej tytuł V rozdziały 4 i 5 odnoszących się do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, Trybunał Sprawiedliwości Unii Europejskiej nie jest właściwy w zakresie kontroli ważności lub proporcjonalności działań policji lub innych organów ścigania w Państwie Członkowskim ani do orzekania w sprawie wykonywania przez Państwa Członkowskie obowiązków dotyczących utrzymania porządku publicznego i ochrony bezpieczeństwa wewnętrznego";

([1]) Wyrok z dnia 18 maja 1982 r. w sprawie C-155, AM & S Europe Limited przeciwko Komisji Wspólnot Europejskich.

Z. mając na uwadze, że „bezpieczeństwo narodowe", „bezpieczeństwo wewnętrzne", „bezpieczeństwo wewnętrzne UE" oraz „bezpieczeństwo międzynarodowe" to pojęcia o pokrywających się zakresach znaczeniowych; mając na uwadze, że Konwencja wiedeńska o prawie traktatów, zasada lojalnej współpracy państw członkowskich UE oraz wynikająca z przepisów dotyczących praw człowieka zasada zawężonej interpretacji wyłączeń nakazują zawężoną interpretację pojęcia „bezpieczeństwa narodowego" i wymagają, aby państwa członkowskie wstrzymywały się od wkraczania w kompetencje UE;

AA. mając na uwadze, że Traktaty Europejskie czynią Komisję Europejską „strażniczką Traktatów", a przez to zadaniem Komisji Europejskiej jest wyjaśnianie wszelkich potencjalnych naruszeń unijnego prawa;

AB. mając na uwadze, że zgodnie z art. 6 TUE, dotyczącym Karty praw podstawowych Unii Europejskiej oraz europejskiej konwencji praw człowieka (EKPC), agencje państw członkowskich, a nawet podmioty prywatne działające w dziedzinie bezpieczeństwa narodowego, muszą również szanować zapisane tam prawa, niezależnie od tego, czy kwestia dotyczy obywateli danego państwa czy obywateli innych państw;

Eksterytorialność

AC. mając na uwadze, że eksterytorialne zastosowanie przez państwa trzecie właściwych im przepisów ustawowych, wykonawczych oraz innych instrumentów ustawodawczych lub wykonawczych należących do jurysdykcji UE lub państw członkowskich może wpływać na ustanowiony porządek prawny oraz praworządność, a nawet naruszać prawo międzynarodowe lub unijne, w tym prawa osób fizycznych i prawnych, biorąc pod uwagę zakres i zadeklarowany lub faktyczny cel takiego zastosowania; mając na uwadze, że w tych okolicznościach konieczne jest podjęcie na szczeblu UE działań mających na celu zapewnienie poszanowania na terytorium UE unijnych wartości zapisanych w art. 2 TUE, w Karcie praw podstawowych Unii Europejskiej i w EKPC, tj. praw podstawowych, demokracji oraz praworządności, a także praw osób fizycznych i prawnych zapisanych w ustawodawstwie wtórnym wdrażającym te fundamentalne zasady, w szczególności przez usunięcie, zneutralizowanie, zablokowanie lub zwalczanie w inny sposób skutków odnośnego ustawodawstwa zagranicznego;

Międzynarodowe transfery danych

AD. mając na uwadze, że transfer danych osobowych przez unijne instytucje, organy, urzędy lub agencje, lub przez państwa członkowskie do Stanów Zjednoczonych w celach związanych z egzekwowaniem prawa w sytuacji braku odpowiednich zabezpieczeń i ochrony poszanowania praw podstawowych obywateli UE, w szczególności prawa do prywatności i ochrony danych osobowych, sprawiłby, że dana instytucja unijna, unijny organ, urząd, unijna agencja lub państwo członkowskie ponosiłyby na mocy art. 340 TFUE lub orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej ([1]) odpowiedzialność za naruszenie prawa unijnego, w tym naruszenie praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej;

AE. mając na uwadze, że przekazywanie danych nie jest ograniczone geograficznie, i szczególnie w kontekście postępującej globalizacji i ogólnoświatowej łączności ustawodawca UE ma do czynienia z nowymi wyzwaniami w zakresie ochrony danych osobowych i łączności, mając na uwadze, że niezwykle ważne jest zatem promowanie ram prawnych opartych wspólnych norm;

AF. mając na uwadze, że masowe gromadzenie danych osobowych w celach handlowych oraz w ramach walki z terroryzmem i poważną przestępczością transnarodową stanowi zagrożenie dla danych osobowych oraz do prywatności obywateli UE;

Transfery do Stanów Zjednoczonych realizowane w oparciu o zasady bezpiecznego transferu danych osobowych (w ramach „bezpiecznej przystani")

AG. mając na uwadze, że amerykańskie ramy prawne dotyczące ochrony danych osobowych nie gwarantują odpowiedniego poziomu ochrony obywatelom UE;

AH. mając na uwadze, że w celu umożliwienia unijnym administratorom danych dokonania transferu danych osobowych do podmiotu ze Stanów Zjednoczonych Komisja w swojej decyzji 2000/520/WE ogłosiła adekwatność ochrony przewidzianej przez zasady bezpiecznego transferu danych osobowych oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA w odniesieniu do danych osobowych przekazywanych z Unii do organizacji z siedzibą w Stanach Zjednoczonych, które zgodziły się przestrzegać zasad bezpiecznego transferu danych osobowych;

([1]) Zob. szczególnie sprawy połączone C-6/90 i C-9/90, Francovich i in. przeciwko Włochom, wyrok z dnia 19 listopada 1991 r.

AI. mając na uwadze, że w swej rezolucji z dnia 5 lipca 2000 r. Parlament wyraził wątpliwości i obawy co do adekwatności zasad bezpiecznego transferu danych osobowych i wezwał Komisję do odpowiednio szybkiej zmiany decyzji w kontekście doświadczeń oraz wszelkich postępów ustawodawczych;

AJ. mając na uwadze dokument roboczy Parlamentu nr 4 z dnia 12 grudnia 2013 r. w sprawie amerykańskich działań w zakresie nadzoru w odniesieniu do danych unijnych oraz możliwych prawnych implikacji takich działań dla umów transatlantyckich i współpracy transatlantyckiej, w którym sprawozdawcy wyrazili wątpliwości i obawy dotyczące adekwatności programu bezpiecznego transferu danych osobowych i wezwali Komisję do uchyleniu decyzji o adekwatności zasad bezpiecznego transferu danych osobowych oraz do znalezienia nowych rozwiązań prawnych;

AK. mając na uwadze, że decyzja Komisji 2000/520/WE stanowi, iż właściwe organy w państwach członkowskich mogą wykorzystywać swe obecne uprawnienia do zawieszenia przepływu danych do organizacji, która zadeklarowała się przestrzegać zasad bezpiecznego transferu danych osobowych w celu ochrony jednostek w związku z przetwarzaniem ich danych osobowych, w przypadku gdy istnieje zasadnicze prawdopodobieństwo, że dochodzi do naruszania zasad bezpiecznego transferu danych osobowych lub że dalsze dokonywanie transferu łączyłoby się z nieuniknionym ryzykiem poważnej szkody podmiotów danych;

AL. mając na uwadze, że w decyzji Komisji 2000/520/WE mowa również o tym, iż w przypadku dostarczenia dowodów wskazujących na to, że osoba odpowiedzialna za zapewnienie zgodności działań z zasadami nie wypełnia swojej roli, Komisja musi poinformować o tym Departament Handlu USA oraz, w stosownych przypadkach, przedstawić środki mające na celu wycofanie lub zawieszenie danej decyzji lub ograniczenie zakresu jej stosowania;

AM. mając na uwadze, że w swych pierwszych dwóch sprawozdaniach w sprawie wdrożenia zasad bezpiecznego transferu danych osobowych, z 2002 r. i 2004 r., Komisja stwierdziła szereg uchybień w kwestii właściwego wdrożenia zasad bezpiecznego transferu danych osobowych i sformułowała szereg zaleceń dla władz amerykańskich służących naprawie tych uchybień;

AN. mając na uwadze, że w trzecim sprawozdaniu z realizacji z dnia 27 listopada 2013 r., które sporządzono dziewięć lat po drugim sprawozdaniu, stwierdzono, iż żadne z uchybień opisanych w poprzednim sprawozdaniu nie zostało naprawione, a Komisja stwierdziła kolejne liczne słabości i niedociągnięcia w realizacji zasad bezpiecznego transferu danych osobowych i postanowiła, że dalsza realizacja w obecnym kształcie jest niemożliwa; mając na uwadze, że Komisja podkreślała, iż szeroki dostęp amerykańskich agencji wywiadu do danych przekazywanych do Stanów Zjednoczonych przez podmioty, które zaakceptowały zasady bezpiecznego transferu danych osobowych, budzi dodatkowe poważne wątpliwości dotyczące ciągłości ochrony danych osobowych podmiotów danych z Unii Europejskiej; mając na uwadze, że Komisja przedstawiła władzom amerykańskim 13 zaleceń i podjęła się znalezienia do lata 2014 r., wraz z władzami amerykańskimi, środków naprawczych, które miałyby zostać wdrożone możliwie jak najszybciej i które stanowiłoby podstawę pełnego przeglądu funkcjonowania zasad bezpiecznego transferu danych osobowych;

AO. mając na uwadze, że w dniach 28-31 października 2013 r. delegacja Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego spotkała się w Waszyngtonie z przedstawicielami Departamentu Handlu USA oraz amerykańskiej Federalnej Komisji Handlu; mając na uwadze, że Departament Handlu potwierdził istnienie organizacji, które zadeklarowały przestrzeganie zasad bezpiecznego transferu danych, przy czym wyraźnie nie dotrzymują tej deklaracji, co oznacza, że spółki te nie spełniają wymogów określonych w zasadach bezpiecznego transferu danych osobowych pomimo, że dalej otrzymują dane osobowe od UE; mając na uwadze, że Federalna Komisja Handlu przyznała, że zasady bezpiecznego transferu danych osobowych wymagają zmian służących ich udoskonaleniu, szczególnie w kwestii systemu skarg oraz pozasądowego rozstrzygania sporów;

AP. mając na uwadze, że zasady bezpiecznego transferu danych osobowych mogą być ograniczone „w zakresie niezbędnym do spełnienia wymogów bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa"; mając na uwadze, że wyjątek stanowiący odejście od praw podstawowych musi być zawsze interpretowany restrykcyjnie i ograniczony do tego, co niezbędne i proporcjonalne w społeczeństwie demokratycznym, a prawo musi w sposób jasny określać warunki i zabezpieczenia sankcjonujące takie ograniczenie; mając na uwadze, że zakres zastosowania takiego wyjątku powinien być doprecyzowany przez USA i UE, szczególnie przez Komisję, w celu uniknięcia interpretacji lub realizacji, która zasadniczo oznaczałaby unieważnienie praw podstawowych, między innymi praw w zakresie prywatności i ochrony danych; mając na uwadze, że w rezultacie taki wyjątek nie powinien być stosowany w sposób umniejszający znaczenie ochrony zapewnianej na mocy Karty praw podstawowych Unii Europejskiej, EKPC, unijnych przepisów dotyczących ochrony danych osobowych oraz zasad bezpiecznego transferu danych ani w sposób unieważniający taką ochronę; nalega, aby w przypadku powoływania się na wyjątek uzasadniany bezpieczeństwem narodowym konieczne było wskazanie odnośnego przepisu prawa krajowego;

AQ. mając na uwadze, że szeroki dostęp agencji wywiadu Stanów Zjednoczonych poważnie naruszył zaufanie transatlantyckie i wpłynął negatywnie na poziom zaufania wobec organizacji amerykańskich działających na terytorium UE; mając na uwadze, że sytuację dodatkowo utrudnia brak w prawie amerykańskim środków sądowych i administracyjnych umożliwiających dochodzenie roszczeń przez obywateli UE, szczególnie w przypadku działań w zakresie nadzoru prowadzonych w celach wywiadowczych;

Transfery do państw trzecich a decyzja w sprawie odpowiedniej ochrony danych osobowych

AR. mając na uwadze, że zgodnie z ujawnionymi informacjami i ustaleniami procedury dochodzeniowej przeprowadzonej przez komisję LIBE, agencje bezpieczeństwa narodowego Nowej Zelandii, Kanady i Australii były zaangażowane w prowadzony na masową skalę nadzór łączności elektronicznej, aktywnie współpracowały ze Stanami Zjednoczonymi w ramach tzw. sojuszu pięciorga oczu i mogły wymieniać się między sobą danymi osobowymi obywateli UE przekazywanymi z UE;

AS. mając na uwadze, że w decyzjach Komisji 2013/65/UE ([1]) i 2002/2/WE ([2]) określono, że poziom ochrony przewidywany przez nowozelandzką i kanadyjską ustawę o ochronie informacji osobowych i dokumentów elektronicznych jest odpowiedni; mając na uwadze, że wspomniane wcześniej doniesienia podważyły poważnie również zaufanie względem systemów prawnych tych państw w kwestii ciągłości ochrony zapewnianej obywatelom UE; mając na uwadze, że Komisja nie zbadała tego aspektu;

Transfery dokonywane w oparciu o klauzule umowne i inne instrumenty

AT. mając na uwadze, że dyrektywa 95/46/WE stanowi, iż międzynarodowe transfery danych do państwa trzeciego mogą również odbywać się przy wykorzystaniu konkretnych instrumentów, w ramach których administrator danych powołuje się na adekwatne zabezpieczenia dotyczące ochrony prywatności i praw podstawowych oraz wolności jednostek, a także wykonania odnośnych praw;

AU. mając na uwadze, że takie zabezpieczenia mogą w szczególności wynikać z odpowiednich klauzul umownych;

AV. mając na uwadze, że na mocy dyrektywy 95/46/WE Komisja jest uprawniona do podjęcia decyzji o tym, że konkretna standardowa klauzula umowna zapewnia wystarczające zabezpieczenia wymagane tą dyrektywą, oraz mając na uwadze, że na tej podstawie Komisja przyjęła trzy modele standardowych klauzul umownych na potrzeby transferu danych do administratorów i przetwarzających dane (lub podwykonawców przetwarzających) w państwach trzecich;

AW. mając na uwadze, że decyzje Komisji ustanawiające standardowe klauzule umowne stanowią, iż właściwe organy w państwach członkowskich mogą wykorzystywać przysługujące im uprawnienia do wstrzymania przepływu danych, gdy okaże się, że przepisy, którym podlega odbierający dane lub podwykonawca przetwarzający, nakładają na niego obowiązek odstąpienia od obowiązujących przepisów ochrony danych w zakresie wykraczającym poza ograniczenia niezbędne w społeczeństwie demokratycznym zgodnie z art. 13 dyrektywy 95/46/WE, w przypadku gdy wymogi te z dużym prawdopodobieństwem będą w istotny sposób negatywnie wpływać na gwarancje zapewnione obowiązującymi przepisami w zakresie ochrony danych osobowych oraz standardowymi klauzulami umownymi lub gdy istnieje znaczące prawdopodobieństwo, że standardowe klauzule umowne w załączniku nie są lub nie będą przestrzegane, a kontynuowanie transferu danych oznaczałoby nieuniknione ryzyko poważnej szkody podmiotów danych;

AX. mając na uwadze, że krajowe organy ds. ochrony danych opracowały wiążące reguły korporacyjne w celu ułatwienia międzynarodowych transferów w ramach wielonarodowych korporacji, zakładające adekwatne zabezpieczenia dotyczące ochrony prywatności i praw podstawowych oraz wolności jednostek, a także egzekwowania odnośnych praw; mając na uwadze, że wiążące reguły korporacyjne muszą być przed rozpoczęciem ich stosowania zatwierdzone przez właściwe organy państw członkowskich, które najpierw stwierdzają ich zgodność z unijnymi przepisami w zakresie ochrony danych osobowych; mając na uwadze, że wiążące reguły korporacyjne dla przetwarzających dane zostały odrzucone w sprawozdaniu Komisji LIBE w sprawie ogólnego rozporządzenia o ochronie danych, ponieważ sprawiłyby, że administrator danych oraz podmiot danych nie mieliby żadnej kontroli nad jurysdykcją, w której przetwarzane są dane;

([1]) Dz.U. L 28 z 30.1.2013, s. 12.
([2]) Dz.U. L 2 z 4.1.2002, s. 13.

AY. mając na uwadze, że Parlament Europejski, z racji swoich kompetencji określonych w art. 218 TFUE, ma obowiązek nieustannego monitorowania wartości umów międzynarodowych, na które wyraził zgodę;

Transfery dokonywane w oparciu o umowy w sprawie TFTP i PNR

AZ. mając na uwadze, że w swojej rezolucji z dnia 23 października 2013 r. Parlament wyraził poważne obawy dotyczące doniesień na temat działalności NSA odnośnie do bezpośredniego dostępu do powiadomień o płatnościach oraz powiązanych danych, co stanowiłoby jawne naruszenie Umowy w sprawie TFTP, w szczególności jej art. 1;

BA. mając na uwadze, że śledzenie środków finansowych należących do terrorystów to kluczowe narzędzie stosowane przy zwalczaniu finansowania terroryzmu oraz poważnej przestępczości, umożliwiające śledczym przeciwdziałającym terroryzmowi odkrywanie połączeń między osobami objętymi śledztwem a potencjalnymi podejrzanymi powiązanymi z bardziej rozległymi siatkami terrorystycznymi podejrzewanymi o finansowanie terroryzmu;

BB. mając na uwadze, że Parlament Europejski zwrócił się do Komisji o zawieszenie Umowy i zażądał, aby wszystkie odnośne informacje i dokumenty zostały niezwłocznie udostępnione na potrzeby obrad parlamentarnych; mając na uwadze, że Komisja nie uczyniła żadnego z powyższych;

BC. mając na uwadze, że w następstwie zarzutów publikowanych przez media Komisja postanowiła rozpocząć konsultacje ze Stanami Zjednoczonymi zgodnie z art. 19 umowy w sprawie TFTP; mając na uwadze, że dnia 27 listopada 2013 r. komisarz Cecilia Malmström poinformowała komisję LIBE, że po spotkaniu z władzami amerykańskimi oraz zapoznaniu się z odpowiedziami udzielonymi przez władze amerykańskie w przesłanych pismach oraz w trakcie spotkań Komisja podjęła decyzję o zakończeniu konsultacji ze względu na brak przesłanek wskazujących, że rząd amerykański działał w sposób niezgodny z postanowieniami Umowy, a także mając na uwadze, że Stany Zjednoczone złożyły pisemne oświadczenie, w którym zapewniają, że nie miało miejsca żadne bezpośrednie gromadzenie danych niezgodne z postanowieniami umowy w sprawie TFTP; mając na uwadze, że nie ma jasności co do tego, czy władze amerykańskie obeszły Umowę, uzyskując dostęp do takich danych przy użyciu innych środków, o czym świadczy wystosowane przez władze amerykańskie pismo z dnia 18 września 2013 r. ([1]);

BD. mając na uwadze, że podczas pobytu delegacji LIBE w Waszyngtonie w dniach 28–31 października 2013 r. członkowie delegacji spotkali się z przedstawicielami Departamentu Skarbu USA; mając na uwadze, że przedstawiciele Departamentu Skarbu USA stwierdzili, że od chwili wejścia w życie umowy w sprawie TFTP nie mieli dostępu do danych SWIFT w UE, z wyjątkiem przypadków przewidzianych umową w sprawie TFTP; mając na uwadze, że Departament Skarbu USA odmówił komentarza na temat tego, czy dane SWIFT były pozyskiwane poza ramami umowy w sprawie TFTP przez inny amerykański organ rządowy lub departament oraz czy administracja Stanów Zjednoczonych była świadoma prowadzonych przez NSA działań w zakresie prowadzonego na masową skalę nadzoru; mając na uwadze, że dnia 18 grudnia 2013 r. Glenn Greenwald stwierdził w dochodzeniu prowadzonym przez LIBE, że NSA i GCHQ ukierunkowywały swoje działania na sieci SWIFT;

BE. mając na uwadze, że dnia 13 listopada 2013 r. belgijskie i niderlandzkie organy ochrony danych podjęły decyzję o przeprowadzeniu wspólnego dochodzenia w sprawie bezpieczeństwa sieci płatności SWIFT w celu upewnienia się, czy osoby trzecie mogły uzyskać niedozwolony lub bezprawny dostęp do informacji bankowych obywateli UE ([2]);

BF. mając na uwadze, że zgodnie ze wspólnym przeglądem zawartej między UE a USA umowy w sprawie PNR, Departament Bezpieczeństwa Wewnętrznego USA 23 razy ujawnił NSA dane PNR na potrzeby przypadków zwalczania terroryzmu, a wszystko odbywało się zgodnie ze szczegółowymi warunkami Umowy;

BG. mając na uwadze, że we wspólnym przeglądzie nie wspomniano o tym, iż w przypadku przetwarzania danych osobowych do celów wywiadowczych w świetle prawa amerykańskiego osobom spoza USA nie przysługuje sądowa ani administracyjna ścieżka umożliwiająca ochronę przysługujących praw, a ochrona wynikająca z konstytucji obejmuje jedynie osoby ze Stanów Zjednoczonych; mając na uwadze, że taki brak praw sądowych lub administracyjnych unieważnia ochronę obywateli UE, o której mowa w istniejącej umowie w sprawie PNR;

([1]) W piśmie stwierdzono, że „rząd Stanów Zjednoczonych wyszukuje i pozyskuje informacje finansowe […] (które) są gromadzone w ramach kanałów regulacyjnych, procedur egzekwowania prawa, kanałów dyplomatycznych oraz wywiadowczych, a także w drodze wymiany z partnerami zagranicznymi […]" oraz że „rząd Stanów Zjednoczonych wykorzystuje program śledzenia środków finansowych należących do terrorystów do uzyskania danych SWIFT, których nie uzyskujemy z innych źródeł";

([2]) http://www.privacycommission.be/fr/news/les-instances-europ%C3%A9ennes-charg%C3%A9es-de-contr%C3%B4ler-le-respect-de-la-vie-priv%C3%A9e-examinent-la

Transfery dokonywane w oparciu o zawarte przez UE i USA porozumienie o wzajemnej pomocy prawnej w sprawach karnych

BH. mając na uwadze porozumienie między Unią Europejską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej w sprawach karnych z dnia 6 czerwca 2003 r. ([1]), które weszło w życia dnia 1 lutego 2010 r. i ma ułatwić współpracę między UE a USA w celu skuteczniejszego zwalczania przestępczości z należytym poszanowaniem praw jednostek oraz rządów prawa;

Umowa ramowa w sprawie ochrony danych osobowych w dziedzinie współpracy policyjnej i sądowej (tzw. umowa parasolowa)

BI. mając na uwadze, że celem tej ogólnej umowy jest stworzenie ram prawnych odnoszących się do wszystkich transferów danych osobowych dokonywanych między UE a USA wyłącznie na potrzeby działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych, w tym terroryzmu, w ramach współpracy policyjnej i sądowej w sprawach karnych; mając na uwadze, że Rada wydała zezwolenie na negocjacje w dniu 2 grudnia 2010 r.; mając na uwadze, że umowa ta ma ogromne znaczenie, ponieważ stanowiłaby ona podstawę ułatwienia transferu danych w kontekście współpracy policyjnej i sądowej oraz w kontekście spraw karnych;

BJ. mając na uwadze, że umowa ta powinna jasno i precyzyjnie określać prawnie wiążące zasady przetwarzania danych, a w szczególności powinna uznawać prawo obywateli UE do sądowego dostępu do danych, korekty danych oraz usuwania danych osobowych na terytorium Stanów Zjednoczonych, jak również prawo do skutecznego administracyjnego i sądowego mechanizmu dochodzenia roszczeń przysługującego obywatelom UE w USA, powinna ona także przewidywać niezależny nadzór czynności związanych z przetwarzaniem danych;

BK. mając na uwadze, że w swoim komunikacie z dnia 27 listopada 2013 r. Komisja zaznaczyła, że umowa parasolowa powinna skutkować wysokim poziomem ochrony obywateli po obu stronach Oceanu Atlantyckiego oraz powinna wzmocnić zaufanie Europejczyków do wymiany danych między UE a USA, zapewniając podstawę dalszego rozwoju unijno-amerykańskiej współpracy i partnerstwa;

BL. mając na uwadze, że negocjacje w sprawie umowy nie posunęły się naprzód, ponieważ rząd Stanów Zjednoczonych niezmiennie odmawia uznania skutecznych praw w zakresie administracyjnego i sądowego dochodzenia roszczeń przez obywateli UE, a także ze względu na zamiar stosowania szerokich odstępstw od zasad ochrony danych osobowych zawartych w umowie, takich jak ograniczenie celowe, zatrzymywanie danych lub dalsze transfery w kraju lub za granicą;

Reforma ochrony danych

BM. mając na uwadze, że unijne ramy prawne w zakresie ochrony danych osobowych są obecnie przedmiotem przeglądu prowadzonego w celu stworzenia kompleksowego, spójnego, nowoczesnego i stabilnego systemu prowadzenia wszelkich czynności związanych z przetwarzaniem danych na terytorium Unii; mając na uwadze, że w styczniu 2012 r. Komisja przedstawiła pakiet wniosków ustawodawczych: ogólne rozporządzenie o ochronie danych ([2]), które zastąpi dyrektywę 95/46/WE i wprowadzi jednolite przepisy w całej UE, a także dyrektywę ([3]) ustanawiającą ujednolicone ramy prawne dotyczące wszelkich czynności w zakresie przetwarzania danych prowadzonych przez organy ścigania do celów egzekwowania prawa oraz ograniczającą obecne rozbieżności ustawodawstw krajowych;

BN. mając na uwadze, że dnia 21 października 2013 r. komisja LIBE przyjęła sprawozdania ustawodawcze dotyczące dwóch wspomnianych wniosków oraz decyzji w sprawie rozpoczęcia negocjacji z Radą w celu przyjęcia instrumentów prawnych podczas bieżącej kadencji;

BO. mając na uwadze, że chociaż Rada Europejska podczas posiedzenia w dniach 24-25 października 2013 r. wezwała do terminowego przyjęcia zdecydowanych unijnych ram ogólnych dotyczących ochrony danych osobowych w celu poprawy zaufania obywateli i przedsiębiorstw do gospodarki cyfrowej, Rada po dwóch latach obrad nadal nie jest w stanie osiągnąć ogólnego stanowiska w kwestii ogólnego rozporządzenia i dyrektywy o ochronie danych ([4]);

([1]) Dz.U. L 181 z 19.7.2003, s. 25.
([2]) COM(2012)0011 z 25.1.2012.
([3]) COM(2012)0010 z 25.1.2012.
([4]) http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/PL/ec/139205.pdf

Bezpieczeństwo informatyczne i przetwarzanie w chmurze obliczeniowej

BP. mając na uwadze, że w wyżej wymienionej rezolucji z dnia 10 grudnia 2013 r. podkreślono potencjał gospodarczy sektora chmury obliczeniowej dla wzrostu gospodarczego i zatrudnienia; mając na uwadze, że ogólną wartość gospodarczą przewiduje się na 207 mld USD rocznie do roku 2016, lub że wartość ta podwoi się do 2012 r.;

BQ. mając na uwadze, że poziom ochrony w środowisku chmury obliczeniowej nie może być niższy niż wymagany w innych kontekstach przetwarzania danych; mając na uwadze, że unijne przepisy dotyczące ochrony danych osobowych, ponieważ są sformułowane w sposób neutralny technologicznie, odnoszą się w pełni również do usług w chmurze obliczeniowej świadczonych w UE;

BR. mając na uwadze, że działalność w zakresie prowadzonego na masową skalę nadzoru daje agencjom wywiadu dostęp do danych osobowych przechowywanych lub w inny sposób przetwarzanych przez osoby z UE w ramach umów o usługi w chmurze zawieranych z głównymi amerykańskimi dostawcami chmury obliczeniowej; mając na uwadze, że amerykańskie służby wywiadowcze miały dostęp do danych osobowych przechowywanych na serwerach znajdujących się na terytorium Unii lub przetwarzały je poprzez podpięcie się do wewnętrznych sieci Yahoo i Google; mając na uwadze, że takie działania stanowią naruszenie zobowiązań międzynarodowych oraz europejskich norm w zakresie praw podstawowych, w tym prawa do życia prywatnego i rodzinnego, poufności komunikacji, domniemania niewinności, wolności wypowiedzi, wolności informacji, wolności zrzeszania się i zgromadzeń, a także wolności prowadzenia działalności gospodarczej; mając na uwadze, że nie można wykluczyć, iż służby wywiadowcze miały również dostęp do informacji przechowywanych w chmurze przez organy publiczne państw członkowskich lub przedsiębiorstwa i instytucje;

BS. mając na uwadze, że w agencjach wywiadu obowiązuje polityka systematycznie podważająca protokoły szyfrowania i produkty szyfrujące w celu uzyskania możliwości przechwytywania komunikacji, nawet gdy jest ona szyfrowana; mając na uwadze, że NSA zgromadziła ogromną ilość tzw. luk zero-day – słabości zabezpieczeń teleinformatycznych, o których nie wie jeszcze opinia publiczna ani sprzedawca produktu; mając na uwadze, że takie działania poważnie podważają ogólnoświatowe wysiłki na rzecz poprawy bezpieczeństwa teleinformatycznego;

BT. mając na uwadze, że fakt posiadania przez agencje wywiadu dostępu do danych osobowych użytkowników usług internetowych poważnie naruszył zaufanie obywateli do takich usług, a przez to ma negatywny wpływ na przedsiębiorstwa inwestujące w rozwój nowych usług wykorzystujących technologię dużych zbiorów danych oraz nowe zastosowania, takie jak internet przedmiotów;

BU. mając na uwadze, że sprzedawcy IT często dostarczają produkty, które nie zostały właściwie przetestowane pod względem bezpieczeństwa lub nawet takie, do których sprzedawca celowo wprowadził lukę typu backdoor; mając na uwadze, że brak zasad dotyczących odpowiedzialności ponoszonej przez sprzedawców oprogramowania doprowadził do sytuacji, którą wykorzystują z kolei agencje wywiadu, a która jednocześnie stwarza ryzyko ataku ze strony innych podmiotów;

BV. mając na uwadze, że kwestią kluczową dla przedsiębiorstw świadczących nowe usługi i oferujących nowe zastosowania jest poszanowanie zasad ochrony danych osobowych oraz prywatności podmiotów danych, których dane są gromadzone, przetwarzane i analizowane, aby możliwe było utrzymanie wysokiego poziomu zaufania obywateli;

Demokratyczny nadzór nad służbami wywiadowczymi

BW. mając na uwadze, że służbom wywiadowczym w społeczeństwach demokratycznych udzielono specjalnych uprawnień i zapewniono im możliwości ochrony praw podstawowych, demokracji oraz rządów prawa, praw obywateli i państwa przed poważnymi zagrożeniami wewnętrznymi i zewnętrznymi, podlegają one również kontroli sądowej oraz rozliczalności demokratycznej; mając na uwadze, że służby te dysponują szczególnymi uprawnieniami i możliwościami wyłącznie w tym zakresie; mając na uwadze, że uprawnienia te powinny być wykorzystywane w ramach granic prawnych wyznaczonych prawami podstawowymi, demokracją i praworządnością, zaś ich stosowanie powinno podlegać skrupulatnej kontroli, w przeciwnym wypadku służby tracą legitymizację oraz ryzykują podważeniem demokracji;

BX. mając na uwadze fakt, że dozwolony jest pewien stopień poufności w przypadku służb wywiadowczych z uwagi na potrzebę uniknięcia narażania prowadzonych operacji, ujawnienia trybu funkcjonowania służb lub zagrożenia życia agentów, przy czym poufność taka nie może być nadrzędna w stosunku do zasad demokratycznej i sądowej kontroli i inspekcji ich działalności, jak również przejrzystości lub ich wyłączać, szczególnie jeżeli chodzi o poszanowanie praw podstawowych i praworządności, które stanowią podwaliny społeczeństwa demokratycznego;

BY. mając na uwadze, że większość istniejących krajowych mechanizmów oraz organów nadzoru utworzono lub zrekonstruowano w latach 90. XX w. i niekoniecznie przystosowano je do gwałtownego rozwoju politycznego i technologicznego, jaki można było zaobserwować w ostatnim dziesięcioleciu, a który doprowadził do aktywniejszej międzynarodowej współpracy wywiadu, która obejmuje także wymianę danych osobowych na wielką skalę, jak również do zatarcia granicy dzielącej wywiad i działania w zakresie egzekwowania prawa;

BZ. mając na uwadze, że demokratyczny nadzór nad działaniami wywiadowczymi jest w dalszym ciągu prowadzony wyłącznie na szczeblu krajowym, pomimo rosnącej wymiany informacji między państwami członkowskimi UE oraz między państwami członkowskimi a państwami trzecimi; mając na uwadze, że istnieje coraz większa przepaść między poziomem międzynarodowej współpracy a możliwościami nadzoru ograniczonymi do szczebla krajowego, co skutkuje niewystarczającą i nieskuteczną kontrolą demokratyczną;

CA. mając na uwadze, że krajowe organy nadzoru często nie mają pełnego dostępu do informacji otrzymywanych od zagranicznej agencji wywiadu, co może prowadzić do luk, w których międzynarodowa wymiana informacji może odbywać się bez adekwatnej kontroli; mając na uwadze, że problem ten dodatkowo pogłębia tzw. zasada osoby trzeciej lub zasada kontroli organu zastrzegającego, opracowana z myślą o umożliwieniu organowi zastrzegającemu sprawowania kontroli nad dalszym rozpowszechnianiem należących do niego szczególnie chronionych danych, która to zasada jest jednak niestety często rozumiana jako mająca zastosowanie również do kontroli służb odbiorcy;

CB. mając na uwadze, że prywatne i publiczne inicjatywy reformatorskie na rzecz przejrzystości są kluczowe dla zapewnienia publicznego zaufania do działań agencji wywiadu; mając również na uwadze, że systemy prawne nie powinny uniemożliwiać przedsiębiorstwom ujawniania opinii publicznej informacji na temat sposobu reagowania na wszelkiego rodzaju wnioski rządowe oraz nakazy sądowe dotyczące dostępu do danych użytkownika, w tym możliwości ujawniania zbiorczych zestawień dotyczących liczby wniosków i nakazów w podziale na zrealizowane i odrzucone;

Główne ustalenia

1. uznaje, że ostatnie doniesienia prasowe przekazywane przez osoby zgłaszające przypadki naruszeń oraz dziennikarzy, wraz z zeznaniami ekspertów przedstawionymi podczas prowadzonego dochodzenia, potwierdzenia władz oraz niewystarczająca reakcja na te zarzuty stanowią przekonujący dowód istnienia daleko posuniętych, kompleksowych i zaawansowanych technologicznie systemów stworzonych przez służby wywiadowcze Stanów Zjednoczonych i niektórych państw członkowskich w celu gromadzenia, przechowywania i analizowania danych komunikacyjnych, w tym danych dotyczących treści, lokalizacji oraz metadanych dotyczących wszystkich obywateli na całym świecie na niespotykaną dotąd skalę, w sposób nieograniczony i nieoparty na podejrzeniach;

2. wskazuje szczególnie na programy wywiadowcze amerykańskiej NSA umożliwiające masową inwigilację obywateli UE poprzez bezpośredni dostęp do centralnych serwerów czołowych amerykańskich przedsiębiorstw internetowych (program PRISM), analizę treści oraz metadanych (program Xkeyscore), obchodzenie szyfrowania internetowego (BULLRUN), dostęp do sieci komputerowych i telefonicznych oraz dostęp do danych dotyczących lokalizacji, a także do systemów brytyjskiej agencji wywiadu GCHQ, takich jak nadzór typu upstream (program Tempora) oraz program deszyfrujący (Edgehill), ukierunkowane ataki typu „człowiek pośrodku" (man-in-the-middle) wymierzone w systemy informatyczne (programy Quantumtheory i Foxacid) oraz gromadzenie i przechowywanie 200 mln wiadomości tekstowych dziennie (program Dishfire);

3. odnotowuje doniesienia o rzekomym hakowaniu lub podpinaniu się do systemów Belgacomu przez brytyjską agencję wywiadu GCHQ; odnotowuje oświadczenia Belgacomu, że nie może on potwierdzić ani zaprzeczyć, iż prowadzono działania względem instytucji UE, a także że wykorzystane złośliwe oprogramowanie było niezwykle zaawansowane, a jego opracowanie i zastosowanie wymagało zaangażowania znacznych nakładów finansowych i osobowych, do których dostępu nie miałyby żadne podmioty prywatne ani hakerzy;

4. stwierdza, że poważnie nadwyrężono zaufanie: zaufanie między obydwoma partnerami transatlantyckimi, obywatelami a ich rządami, zaufanie wobec funkcjonowania instytucji demokratycznych po obu stronach Atlantyku, zaufanie do rządów prawa, a także zaufanie względem bezpieczeństwa usług informatycznych i łączności; uważa, że w celu odbudowania zaufania na wszystkich tych płaszczyznach pilnie konieczny jest kompleksowy plan reagowania przewidujący szereg działań podlegających nadzorowi publicznemu;

5. zauważa, że szereg rządów utrzymuje, iż tego typu programy prowadzonego na masową skalę nadzoru są konieczne w celu walki z terroryzmem; zdecydowanie potępia terroryzm, ale jest głęboko przekonany, że walka z terroryzmem nigdy nie może być uzasadnieniem nieukierunkowanych, niejawnych, a czasem nawet niezgodnych z prawem programów prowadzonego na masową skalę nadzoru; jest zdania, że takie programy są niezgodne z zasadami konieczności i proporcjonalności w społeczeństwie demokratycznym;

6. przypomina zdecydowane przekonanie UE o konieczności znalezienia równowagi między środkami bezpieczeństwa a ochroną wolności obywatelskich i praw podstawowych, przy jednoczesnym zapewnieniu jak największego poszanowania prywatności i ochrony danych;

7. uważa, że gromadzenie danych na taką skalę wzbudza znaczne wątpliwości, czy jest ono faktycznie motywowane wyłącznie walką z terroryzmem, ponieważ gromadzeniu podlegają wszelkie możliwe dane na temat wszystkich obywateli; wskazuje zatem na możliwość istnienia innych celów, w tym szpiegostwa politycznego i gospodarczego, którą należy wyeliminować;

8. kwestionuje zgodność działań w zakresie szpiegostwa gospodarczego prowadzonych na masową skalę przez niektóre państwa członkowskie z unijnymi przepisami dotyczącymi rynku wewnętrznego i konkurencji zapisanymi w tytule I oraz tytule VII Traktatu o funkcjonowaniu Unii Europejskiej; potwierdza zasadę lojalnej współpracy zapisaną w art. 4 ust. 3 Traktatu o Unii Europejskiej, oraz zasadę, w myśl której państwa członkowskie „powstrzymują się od podejmowania wszelkich środków, które mogłyby zagrażać urzeczywistnieniu celów Unii";

9. zauważa, że traktaty międzynarodowe oraz prawodawstwo UE i Stanów Zjednoczonych, a także krajowe mechanizmy nadzoru, nie zdołały zagwarantować niezbędnych kontroli i równowagi ani demokratycznej rozliczalności;

10. potępia zakrojone na szeroką skalę, regularne i nieograniczone gromadzenie danych niewinnych osób, często zawierających informacje o bardzo osobistym charakterze; podkreśla, że systemy masowego i nieograniczonego nadzoru prowadzonego przez służby wywiadowcze stanowią poważną ingerencję w prawa podstawowe obywateli; podkreśla, że prywatność nie jest luksusem, ale fundamentem wolnego i demokratycznego społeczeństwa; wskazuje ponadto, że prowadzony na masową skalę nadzór ma potencjalnie poważny wpływ na wolność prasy, myśli i słowa oraz na wolność zrzeszania się i zgromadzeń, a także wiąże się z istotną możliwością niewłaściwego wykorzystywania zgromadzonych informacji przeciwko przeciwnikom politycznym; podkreśla, że działalność w zakresie masowego nadzoru obejmuje również prowadzenie przez służby wywiadowcze działań niezgodnych z prawem i rodzi pytanie o eksterytorialność przepisów krajowych;

11. uważa, że podstawowe znaczenie ma zagwarantowanie ochrony tajemnicy zawodowej prawników, dziennikarzy, lekarzy oraz innych zawodów regulowanych przed działaniami w dziedzinie nadzoru na masowa skalę; podkreśla w szczególności, że wszelka niepewność co do poufności komunikacji pomiędzy prawnikami a ich klientami może negatywnie odbić się na prawie dostępu obywateli UE do porady prawnej, a także dostępu do wymiaru sprawiedliwości oraz prawie do rzetelnego procesu sądowego;

12. postrzega programy nadzoru jako kolejny krok w kierunku stworzenia w pełni prewencyjnego państwa, w którym zmianie ulegnie utrwalony w państwach demokratycznych paradygmat prawa karnego, wskutek czego jakakolwiek ingerencja w prawa podstawowe podejrzanych wymagać będzie zatwierdzenia przez sędziego lub prokuratora na podstawie racjonalnego podejrzenia i uregulowania prawnie, natomiast promowane będzie połączenie egzekwowania prawa i działań wywiadowczych o zatartych i osłabionych zabezpieczeniach prawnych, często niezgodne z kontrolą i równowagą demokratyczną oraz prawami podstawowymi, szczególnie w kwestii domniemania niewinności; przywołuje w związku z tym orzeczenie niemieckiego Federalnego Trybunału Konstytucyjnego ([1]) w sprawie zakazu stosowania siatek prewencyjnych („präventive Rasterfahndung") w sytuacji braku dowodu istnienia konkretnego zagrożenia dla innych, ważnych chronionych przepisami praw, z którego to orzeczenia wynika, że ogólna sytuacja zagrożenia lub napięcia międzynarodowe nie są wystarczającym uzasadnieniem dla stosowania tego typu środków;

13. jest przekonany, że niejawne przepisy i sądy stanowią naruszenie praworządności; zwraca uwagę, że wszelkie wyroki sądu lub trybunału oraz wszelkie decyzje organów administracyjnych państwa nienależącego do UE, zatwierdzające w sposób bezpośredni lub pośredni transfer danych osobowych, nie mogą być w żaden sposób uznawane lub egzekwowane, bez uszczerbku dla układu o wzajemnej pomocy prawnej lub obowiązującej umowy międzynarodowej między wnioskującym państwem trzecim a Unią lub państwem członkowskim i uprzedniego zatwierdzenia przez właściwy organ nadzoru; wskazuje, że wszelkie wyroki tajnego sądu lub trybunału oraz wszelkie decyzje organów administracyjnych państwa nienależącego do UE, zatwierdzające w sposób bezpośredni lub pośredni działania w zakresie nadzoru nie mogą być uznawane lub egzekwowane;

([1]) Nr 1 BvR 518/02 z dnia 4 kwietnia 2006 r.

14. uznaje, że powyższe niepokoje pogłębia szybki rozwój techniki oraz społeczeństwa, jako że internet i urządzenia przenośne są wszechobecne we współczesnym życiu codziennym (wszechobecna informatyzacja), a model biznesowy większości przedsiębiorstw internetowych opiera się na przetwarzaniu danych osobowych; uważa, że skala tego problemu nie ma precedensu; zwraca uwagę, że może to przyczyniać się do powstania sytuacji nadużywania infrastruktury do masowego gromadzenia i przetwarzania danych w przypadkach zmiany systemu politycznego;

15. zauważa, że nie ma żadnej gwarancji, że bezpieczeństwo informatyczne oraz prywatność zarówno unijnych instytucji publicznych, jak i obywateli mogą być w pełni chronione przed ingerencją dobrze wyposażonych intruzów („brak stuprocentowego bezpieczeństwa informatycznego"); zauważa, że aby osiągnąć maksymalne bezpieczeństwo informatyczne, Europejczycy muszą być skłonni przeznaczyć na zachowanie europejskiej niezależności i samowystarczalności w dziedzinie technologii informacyjnej odpowiednie zasoby, zarówno finansowe, jak i personalne;

16. zdecydowanie odrzuca koncepcję mówiącą o tym, iż wszystkie zagadnienia związane z programami prowadzonego na masową skalę nadzoru stanowią wyłącznie kwestię bezpieczeństwa narodowego i w związku z tym należą do wyłącznych kompetencji państw członkowskich; powtórnie apeluje do państw członkowskich, aby, działając na rzecz zapewnienia bezpieczeństwa narodowego, w pełni szanowały prawo UE oraz EKPC; przypomina niedawne rozporządzenie Trybunału Sprawiedliwości, zgodnie z którym „mimo iż to do państw członkowskich należy podjęcie środków zmierzających do zagwarantowania ich bezpieczeństwa zewnętrznego i wewnętrznego, sam tylko fakt, że dana decyzja ma związek z bezpieczeństwem państwa, nie może powodować braku możliwości stosowania prawa Unii" ([1]); przypomina również, że stawką jest tutaj ochrona prywatności wszystkich obywateli UE, a także bezpieczeństwo i wiarygodność wszystkich unijnych sieci łączności; z tego względu uważa, że dyskusja i działanie na szczeblu unijnym są nie tylko uzasadnione, ale są również kwestią autonomii UE;

17. pochwala instytucje i ekspertów, którzy wnieśli wkład w niniejsze dochodzenie; ubolewa nad tym, iż władze kilku państw członkowskich odmówiły współpracy w ramach tego dochodzeniam, które Parlament Europejski prowadzi w imieniu obywateli; z zadowoleniem przyjmuje otwartość niektórych członków Kongresu oraz parlamentów narodowych;

18. ma świadomość, że przy tak ograniczonych ramach czasowych od lipca 2013 r. możliwe było przeprowadzenie jedynie wstępnego rozpoznania wszystkich przedmiotowych kwestii; dostrzega skalę doniesień oraz ich wciąż aktualny charakter; przyjmuje zatem stanowisko przyszłościowe, zakładające zestaw konkretnych propozycji i mechanizmów umożliwiających działania następcze w kolejnej kadencji, co zagwarantuje, że poczynione ustalenia pozostaną ważnym elementem programu politycznego UE;

19. zamierza wezwać do powołania przy nowej Komisji Europejskiej silnych politycznych podmiotów, które zostałyby utworzone po wyborach do Parlamentu Europejskiego w maju 2014 r. w celu zrealizowania propozycji i zaleceń niniejszego dochodzenia;

Zalecenia

20. wzywa władze USA oraz państw członkowskich UE, w których nie ma to jeszcze miejsca, aby zakazały prowadzenia nieograniczonego nadzoru na masową skalę;

21. wzywa państwa członkowskie UE, w szczególności państwa uczestniczące w tzw. sojuszach dziewięciorga i czternaściorga oczu ([2]), do dokonania kompleksowej oceny i w stosownych przypadkach przeglądu przepisów krajowych i praktyk regulujących działalność służb wywiadowczych w celu zagwarantowania, że będą one podlegać nadzorowi sądowemu i publicznemu, że przestrzegają one zasad legalności, konieczności, proporcjonalności, rzetelnego procesu sądowego, powiadamiania użytkowników i przejrzystości, w tym w odniesieniu do kompilacji wzorcowych praktyk ONZ oraz zaleceń Komisji Weneckiej, a także że zachowują one zgodność z normami przewidzianymi europejską konwencją praw człowieka oraz ze zobowiązaniami państw członkowskich w zakresie praw podstawowych, szczególnie w zakresie ochrony danych osobowych, prywatności i domniemania niewinności;

([1]) Wyrok w Sprawie C-300/11, ZZ przeciwko Secretary of State for the Home Department, 4 czerwca 2013 r.

([2]) Tzw. program dziewięciorga oczu obejmuje USA, Zjednoczone Królestwo, Kanadę, Australię, Nową Zelandię, Danię, Francję, Norwegię i Niderlandy. Program czternaściorga oczu obejmuje ww. kraje, a także Niemcy, Belgię, Włochy, Hiszpanię i Szwecję.

22. wzywa wszystkie państwa członkowskie UE, a w szczególności – mając na uwadze swą rezolucje z 4 lipca 2013 r. oraz przesłuchania prowadzone w ramach dochodzenia – Wielką Brytanię, Francję, Niemcy, Szwecję, Niderlandy i Polskę do zagwarantowania, by ich obowiązujące i przyszłe ramy ustawodawcze oraz mechanizmy nadzoru dotyczące działalności agencji wywiadowczych były zgodne z normami europejskiej konwencji praw człowieka oraz prawodawstwem Unii Europejskiej w dziedzinie ochrony danych; wzywa te państwa członkowskie do wyjaśnienia zarzutów o prowadzenie działalności w zakresie nadzoru na masowa skalę, w tym nadzoru telekomunikacji transgranicznej, nieukierunkowanego nadzoru komunikacji przewodowej, potencjalnych umów pomiędzy służbami wywiadowczymi a przedsiębiorstwami telekomunikacyjnymi dotyczących dostępu do danych osobowych i wymiany tych danych, a także dostępu do kabli transatlantyckich, personelu wywiadowczego USA oraz sprzętu znajdującego się na terytorium UE bez kontroli w procesie prowadzenia nadzoru, oraz ich zgodności z prawodawstwem UE; zwraca się do parlamentów narodowych tych krajów, aby zintensyfikowały współpracę swych organów nadzoru nad służbami wywiadowczymi na szczeblu europejskim;

23. wzywa Zjednoczone Królestwo, w szczególności w kontekście licznych doniesień prasowych dotyczących masowej inwigilacji ze strony służb wywiadowczych GCHQ, do dokonania przeglądu obecnych ram prawnych składających się ze „złożonych zależności" między trzema odrębnymi elementami ustawodawstwa: ustawy o prawach człowieka z 1998 r. (Human Rights Act), ustawy o służbach wywiadowczych z 1994 r. (Intelligence Services Act) oraz ustawy regulującej uprawnienia śledcze z 2000 r. (Regulation of Investigatory Powers Act);

24. odnotowuje przegląd holenderskiej ustawy o służbach wywiadowczych i służbach bezpieczeństwa z 2002 r. (sprawozdanie „komisji Dessensa" z dnia 2 grudnia 2013 r.); popiera zalecenia komisji dokonującej przeglądu, które mają na celu zwiększenie przejrzystości holenderskich służb wywiadowczych oraz usprawnienie kontroli i nadzoru nad nimi; wzywa Niderlandy do powstrzymania się od rozszerzania uprawnień służb wywiadowczych w sposób umożliwiający prowadzenie nieukierunkowanego nadzoru na szeroką skalę także w odniesieniu do przewodowej komunikacji niewinnych obywateli, zwłaszcza mając na uwadze fakt, że jeden z największych punktów wymiany ruchu internetowego na świecie mieści się w Amsterdamie (AMS-IX); wzywa do ostrożności w określaniu kompetencji i zdolności nowej jednostki ds. internetowego wywiadu sygnałów (Joint Sigint Cyber Unit), a także do zachowania ostrożności jeżeli chodzi o obecność i działania pracowników wywiadu Stanów Zjednoczonych na terytorium Niderlandów;

25. wzywa państwa członkowskie, także w przypadkach, gdy są reprezentowane przez swoje agencje wywiadu, aby zaniechały przyjmowania od państw trzecich danych, które zostały zgromadzone niezgodnie z prawem, a także zezwalania rządom lub agencjom państw trzecich na prowadzenie na ich terytorium nadzoru, który jest niezgodny z prawem danego państwa lub nie zapewnia zabezpieczeń zapisanych w instrumentach międzynarodowych lub unijnych, w tym ochrony praw człowieka wynikającej z TUE, EKPC oraz Karty praw podstawowych Unii Europejskiej;

26. wzywa do położenia kresu masowemu przechwytywaniu i przetwarzaniu obrazów z kamer internetowych przez służby specjalne; apeluje do państw członkowskich o dokładne zbadanie, czy, w jaki sposób i w jakim stopniu ich służby specjalne zajmowały się gromadzeniem i przetwarzaniem obrazów z kamer internetowych, a także o usunięcie wszelkich przechowywanych obrazów zgromadzonych w ramach programów masowej inwigilacji;

27. wzywa państwa członkowskie do niezwłocznego zrealizowania wynikającego z europejskiej konwencji praw człowieka nakazu ochrony obywateli przed nadzorem prowadzonym niezgodnie z wymogami, w tym w sytuacji gdy celem nadzoru jest zapewnienie bezpieczeństwa narodowego, jeżeli nadzór jest realizowany przez państwa trzecie lub przez ich własne służby wywiadowcze, a także do zagwarantowania, aby rządy prawa nie były osłabione w wyniku eksterytorialnego stosowania przepisów państwa trzeciego;

28. zachęca sekretarza generalnego Rady Europy do wszczęcia 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";

29. wzywa państwa członkowskie do niezwłocznego podjęcia właściwych kroków, w tym sądowych, przeciwko naruszeniu ich suwerenności, a co za tym idzie – naruszaniu ogólnego międzynarodowego prawa publicznego poprzez stosowanie programów prowadzonego na masową skalę nadzoru; apeluje ponadto do państw członkowskich UE o wykorzystanie wszelkich dostępnych środków międzynarodowych do ochrony praw podstawowych obywateli UE, szczególnie przez wszczęcie międzypaństwowej procedury składania skarg z art. 41 Międzynarodowego paktu praw obywatelskich i politycznych;

30. wzywa państwa członkowskie do ustanowienia skutecznych mechanizmów gwarantujących, że osoby odpowiedzialne za programy (masowej) inwigilacji stanowiące naruszenie zasady praworządności i praw podstawowych obywateli zostaną pociągnięte do odpowiedzialności za tego rodzaju nadużycie władzy;

31. wzywa Stany Zjednoczone do bezzwłocznej zmiany przepisów w celu dostosowania ich do prawa międzynarodowego w taki sposób, aby uznać prywatność i inne prawa obywateli UE, by zapewnić obywatelom UE możliwości sądowego dochodzenia roszczeń, tak aby prawa obywateli UE były traktowane na równi z prawami obywateli Stanów Zjednoczonych, oraz do podpisania dodatkowego protokołu umożliwiającego osobom fizycznym składanie skarg na mocy Międzynarodowego paktu praw obywatelskich i politycznych;

32. w tym kontekście z zadowoleniem przyjmuje uwagi i rozporządzenie prezydenta Stanów Zjednoczonych Baracka Obamy wydane w dniu 17 stycznia 2014 r. i jako krok w kierunku ograniczenia udzielania zezwoleń na wykorzystywanie nadzoru i przetwarzanie danych osobowych na potrzeby bezpieczeństwa narodowego oraz w kierunku równego traktowania przez wspólnotę wywiadów Stanów Zjednoczonych danych osobowych wszystkich osób, niezależnie od ich obywatelstwa i miejsca pobytu; w kontekście relacji UE-USA oczekuje jednak dalszych konkretnych kroków, które przede wszystkim umocnią zaufanie w stosunku do transatlantyckich transferów danych i zapewnią wiążące gwarancje możliwego do wyegzekwowania prawa obywateli UE do prywatności, szczegółowo określonego w niniejszym sprawozdaniu;

33. podkreśla 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 budapesztańska) w sprawie 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 skutkowałoby to 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, mianowicie konwencji Rady Europy nr 108;

34. wzywa Komisję do przeprowadzenia do lipca 2014 r. oceny stosowania rozporządzenia (WE) nr 2271/96 w odniesieniu do przypadków konfliktów przepisów dotyczących transferów danych osobowych;

35. wzywa Agencję Praw Podstawowych Unii Europejskiej do przeprowadzenia szczegółowego badania na temat ochrony praw podstawowych w kontekście nadzoru, a zwłaszcza na temat aktualnej sytuacji prawnej obywateli UE jeżeli chodzi o środki odwoławcze, jakie przysługują im w związku z tymi praktykami;

Międzynarodowe transfery danych

Ramy prawne Stanów Zjednoczonych dotyczące ochrony danych i ich zasady bezpiecznego transferu danych osobowych

36. zauważa, że przedsiębiorstwa określone w doniesieniach medialnych jako zaangażowane w nadzór prowadzony na masową skalę względem podmiotów danych w UE przez NSA Stanów Zjednoczonych są przedsiębiorstwami, które zadeklarowały zgodność z zasadami bezpiecznego transferu danych osobowych, a zasady te są instrumentem prawnym stosowanym przy transferze danych osobowych obywateli UE do Stanów Zjednoczonych (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); wyraża zaniepokojenie tym, że organizacje te przyznały, iż nie szyfrują informacji i komunikacji przepływających między ich centrami danych, tym samym umożliwiając służbom wywiadowczym przechwytywanie informacji; z zadowoleniem przyjmuje wydane następnie przez niektóre przedsiębiorstwa amerykańskie oświadczenia dotyczące przyspieszenia planów wdrażania szyfrowania przepływu danych między ich światowymi centrami danych;

37. uważa, że szeroki dostęp amerykańskich agencji wywiadu do danych osobowych obywateli UE przetwarzanych zgodnie z zasadami bezpiecznego transferu danych osobowych nie spełnia kryteriów umożliwiających odstępstwo ze względów „bezpieczeństwa narodowego”;

38. jest zdania, że ponieważ w obecnych okolicznościach zasady bezpiecznego transferu danych osobowych nie zapewniają odpowiedniej ochrony obywatelom UE, transfery te powinny odbywać się na mocy innych instrumentów, takich jak klauzule umowne lub wiążące reguły korporacyjne określające konkretne środki zabezpieczające i ochronne, pod warunkiem, ze instrumenty te gwarantują odpowiednie zabezpieczenia i ochronę oraz że nie obchodzi się ich za pomocą innych ram prawnych;

39. jest zdania, że Komisja nie podjęła działań, by zaradzić stwierdzonym uchybieniom w kwestii obecnego wdrożenia zasad bezpiecznego transferu danych;

40. wzywa Komisję do przedstawienia środków przewidujących bezzwłoczne zawieszenie decyzji Komisji 2000/520/WE, w której uznano adekwatność zasad bezpiecznego transferu danych osobowych oraz odnoszących się do nich najczęściej zadawanych pytań wydanych przez Departament Handlu USA; wzywa zatem władze USA do wysunięcia wniosku w sprawie nowych ram transferów danych osobowych z UE do USA, który byłby zgodny z unijnymi wymogami w zakresie ochrony danych oraz gwarantowałby odpowiedni poziom ochrony;

41. wzywa właściwe organy państw członkowskich, w szczególności organy odpowiedzialne za ochronę danych, do wykorzystania posiadanych uprawnień i bezzwłocznego zawieszenia przepływów danych do wszelkich organizacji deklarujących zgodność z amerykańskimi zasadami bezpiecznego transferu danych osobowych oraz do określenia wymogu, zgodnie z którym takie przepływy danych mogłyby odbywać się wyłącznie na podstawie innych instrumentów, o ile zawierają one niezbędne środki zabezpieczające i ochronne w odniesieniu do ochrony prywatności oraz podstawowych praw i wolności osób;

42. wzywa Komisję do przedstawienia do grudnia 2014 r. kompleksowej oceny amerykańskich ram ochrony prywatności obejmujących działalność handlową, działania organów ścigania i działania wywiadowcze oraz konkretnych zaleceń w oparciu o brak ogólnego prawa dotyczącego ochrony danych osobowych w Stanach Zjednoczonych; zachęca Komisję do nawiązania współpracy z administracją USA w celu stworzenia ram prawnych gwarantujących wysoki poziom ochrony osób jeżeli chodzi o ochronę ich danych osobowych podczas ich transferu do USA, a także zagwarantowanie równoważności ram unijnych i amerykańskich ram prawnych dotyczących prywatności;

Transfery do innych państw trzecich, wobec których wydano decyzję w sprawie odpowiedniej ochrony danych osobowych

43. przypomina, że dyrektywa 95/46/WE stanowi, iż przekazywanie do państwa trzeciego danych osobowych może nastąpić tylko wówczas, gdy, niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych przepisów dyrektywy, dane państwo trzecie zapewnia odpowiedni poziom ochrony, a celem tego przepisu jest zapewnienie ciągłości ochrony przysługującej na podstawie prawa UE dotyczącego ochrony danych, jeżeli dane osobowe są przekazywane poza UE;

44. przypomina, że dyrektywa 95/46/WE stanowi także, iż odpowiedni poziom ochrony zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji; przypomina również, że wspomniana dyrektywa nadaje także Komisji uprawnienia wykonawcze w zakresie uznania, iż państwo trzecie zapewnia odpowiedni poziom ochrony w świetle kryteriów określonych w dyrektywie 95/46/WE; przypomina, że dyrektywa 95/46/WE uprawnia również Komisję do uznania, że państwo trzecie nie zapewnia odpowiedniego poziomu ochrony;

45. przypomina, że w tym ostatnim przypadku państwa członkowskie muszą podjąć konieczne środki, aby nie dopuścić do przekazania jakichkolwiek danych tego samego rodzaju do danego państwa trzeciego, a Komisja powinna przystąpić do negocjacji w celu zaradzenia sytuacji;

46. wzywa Komisję i państwa członkowskie do bezzwłocznego dokonania oceny, czy na odpowiedni poziom ochrony określony w nowozelandzkiej ustawie o ochronie prywatności kanadyjskiej ustawie o ochronie informacji osobowych i dokumentach elektronicznych, uznany w decyzjach Komisji 2013/65/UE i 2002/2/WE, wpływ miało zaangażowanie krajowych agencji wywiadu tych krajów w nadzór prowadzony na masową skalę względem obywateli UE, a w razie konieczności do przedsięwzięcia stosownych środków w celu zawieszenia lub uchylenia decyzji w sprawie odpowiedniej ochrony danych osobowych; ponadto wzywa Komisję do dokonania oceny sytuacji innych państw, które otrzymały rating zgodności; oczekuje, że Komisja przedstawi Parlamentowi sprawozdanie w sprawie swoich ustaleń na temat wspomnianych powyżej państw najpóźniej do grudnia 2014 r.;

Transfery dokonywane w oparciu o klauzule umowne i inne instrumenty

47. przypomina, że krajowe organy ds. ochrony danych wskazały, iż przy opracowywaniu standardowych klauzul umownych i wiążących reguł korporacyjnych nie uwzględniono sytuacji dostępu do danych osobowych do celów prowadzonego na masową skalę nadzoru oraz że dostęp taki nie byłby zgodny z klauzulami derogacyjnymi zawartymi w klauzulach umownych lub wiążących regułach korporacyjnych, które odnoszą się do wyjątkowych odstępstw ze względów uzasadnionych interesem społeczeństwa demokratycznego, o ile jest to niezbędne i proporcjonalne;

48. wzywa państwa członkowskie do zakazania lub zawieszenia przepływów danych do państw trzecich na podstawie standardowych klauzul umownych, klauzul umownych lub wiążących reguł korporacyjnych, na które zgodę wydały właściwe organy krajowe, w razie prawdopodobieństwa że prawo, któremu podlegają odbiorcy danych, nakłada na nich wymogi wykraczające poza ograniczenia ściśle konieczne, odpowiednie i proporcjonalne w społeczeństwie demokratycznym i mogące wywrzeć niekorzystne skutki na gwarancje zapewnione właściwym prawem dotyczącym ochrony danych i standardowymi klauzulami umownymi lub ze względu na to, że dalszy transfer stwarzałby ryzyko wyrządzenia poważnej szkody podmiotom danych;

49. wzywa Grupę Roboczą Art. 29 do wydania wytycznych i zaleceń dotyczących środków zabezpieczających i ochronnych, które powinny zawierać instrumenty umowne dotyczące międzynarodowego transferu danych osobowych obywateli UE w celu zapewnienia ochrony prywatności, podstawowych praw i wolności osób, biorąc zwłaszcza pod uwagę przepisy państw trzecich dotyczące wywiadu i bezpieczeństwa narodowego oraz udział przedsiębiorstw otrzymujących dane w państwie trzecim w działaniach w zakresie nadzoru prowadzonych na masową skalę przez agencje wywiadu państwa trzeciego;

50. wzywa Komisję do niezwłocznego przeprowadzenia analizy określonych przez nią standardowych klauzul umownych w celu oceny tego, czy zapewniają one niezbędną ochronę w odniesieniu do dostępu do danych osobowych przekazywanych na mocy klauzul do celów wywiadowczych, oraz w stosownym przypadku do ich przeglądu;

Transfery dokonywane w oparciu o porozumienie o wzajemnej pomocy prawnej

51. wzywa Komisję do przeprowadzenia do końca 2014 r. gruntownej oceny obowiązującego porozumienia o wzajemnej pomocy prawnej na mocy jego art. 17 w celu sprawdzenia jego praktycznego stosowania, a zwłaszcza oceny tego, czy Stany Zjednoczone skutecznie wykorzystały porozumienie do uzyskania informacji lub dowodów w UE i czy doszło do jego obejścia w celu uzyskania informacji bezpośrednio w UE, a także do oceny wpływu na prawa podstawowe osób; ocena taka nie powinna odnosić się tylko do oficjalnych oświadczeń Stanów Zjednoczonych jako wystarczającej podstawy analizy, lecz powinna także opierać się na szczegółowych ocenach UE; ten gruntowny przegląd powinien również dotyczyć skutków zastosowania unijnych zasad konstytucyjnych do tego instrumentu w celu dostosowania go do prawa Unii, z uwzględnieniem zwłaszcza jego protokołu nr 36 i art. 10 oraz deklaracji nr 50 dotyczącej tego protokołu; jednocześnie wzywa Radę i Komisję do dokonania oceny dwustronnych umów między państwami członkowskimi a Stanami Zjednoczonymi w celu zapewnienia spójności wspomnianych umów dwustronnych z obecnymi lub przyszłymi umowami między UE a Stanami Zjednoczonymi;

Wzajemna pomoc UE w sprawach karnych

52. zwraca się do Rady i Komisji o poinformowanie Parlamentu o faktycznym zastosowaniu przez państwa członkowskie konwencji o pomocy prawnej w sprawach karnych zawartej między państwami członkowskimi, a zwłaszcza tytułu III dotyczącego przechwytywania przekazów telekomunikacyjnych; wzywa Komisję, aby zgodnie z deklaracją nr 50 przedstawiła do końca 2014 r. wniosek dotyczący protokołu nr 36 w celu dostosowania go do ram określonych Traktatem z Lizbony, o co wnioskowano;

Transfery dokonywane w oparciu o umowy w sprawie TFTP i PNR

53. jest zdania, że informacje podane przez Komisję Europejską i Departament Skarbu USA nie wyjaśniają, czy amerykańskie agencje wywiadu mają dostęp do komunikatów finansowych SWIFT w UE dzięki przechwytywaniu sieci SWIFT albo systemów operacyjnych lub sieci łączności banków, samodzielnie lub we współpracy z krajowymi agencjami wywiadu w UE i bez korzystania z istniejących dwustronnych kanałów wzajemnej pomocy prawnej i współpracy sądowej;

54. odwołuje się do swojej rezolucji z dnia 23 października 2013 r. i zwraca się do Komisji o zawieszenie umowy w sprawie TFTP;

55. wzywa Komisję do zareagowania na obawy, że trzy z największych komputerowych systemów rezerwacji wykorzystywanych przez przewoźników lotniczych na świecie znajdują się w Stanach Zjednoczonych, a dane PNR są zapisywane w systemach opartych na modelu chmury działających na terytorium Stanów Zjednoczonych zgodnie z prawem Stanów Zjednoczonych, które nie zapewnia odpowiedniego poziomu ochrony danych;

Umowa ramowa w sprawie ochrony danych osobowych w dziedzinie współpracy policyjnej i sądowej (tzw. umowa parasolowa)

56. uważa, że zadowalającym rozwiązaniem na podstawie „umowy parasolowej" jest określenie warunku wstępnego pełnego przywrócenia zaufania między partnerami transatlantyckimi;

57. zwraca się o bezzwłoczne wznowienie negocjacji ze Stanami Zjednoczonymi w sprawie „umowy parasolowej", która powinna zapewniać traktowanie praw obywateli UE na równi z prawami obywateli Stanów Zjednoczonych; ponadto podkreśla, że umowa ta powinna przewidywać skuteczne i możliwe do wyegzekwowania administracyjne i sądowe środki odwoławcze dla wszystkich obywateli UE w Stanach Zjednoczonych bez jakiejkolwiek dyskryminacji;

58. zwraca się do Komisji i Rady o to, by do czasu wejścia w życie „umowy parasolowej" nie występowały z inicjatywą zawarcia ze Stanami Zjednoczonymi nowych umów sektorowych lub określenia nowych ustaleń sektorowych dotyczących transferu danych osobowych do celów egzekwowania prawa;

59. wzywa Komisję do przedstawienia szczegółowych informacji na temat poszczególnych elementów mandatu negocjacyjnego oraz aktualnej sytuacji do kwietnia 2014 r.;

Reforma ochrony danych

60. wzywa prezydencję Rady i państwa członkowskie, aby przyspieszyły prace nad całym pakietem dotyczącym ochrony danych w celu umożliwienia jego przyjęcia w 2014 r., tak aby obywatele UE mogli korzystać z wysokiego poziomu ochrony w najbliższej przyszłości; podkreśla, że silne zaangażowanie i pełne poparcie ze strony Rady jest niezbędnym warunkiem pokazania wiarygodności i siły przebicia wobec państw trzecich;

61. 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 przyjmie dalsze środki dotyczące współpracy w dziedzinie egzekwowania prawa dopiero po przystąpieniu przez Radę do negocjacji z Parlamentem i Komisją w sprawie pakietu dotyczącego ochrony danych;

62. przypomina, że koncepcje „uwzględnienia ochrony prywatności już w fazie projektowania" i „domyślnej ochrony prywatności" zwiększają ochronę danych i powinny mieć status wytycznych dla wszystkich produktów, usług i systemów oferowanych w internecie;

63. uważa wyższe normy przejrzystości i bezpieczeństwa w sektorze internetowym i telekomunikacyjnym za zasadę konieczną do poprawy systemu ochrony danych; w związku z tym wzywa Komisję do przedstawienia wniosku ustawodawczego dotyczącego standardowych warunków ogólnych dla usług internetowych i telekomunikacyjnych oraz nadania organowi nadzoru uprawnień do monitorowania przestrzegania warunków ogólnych;

Przetwarzanie w chmurze

64. zauważa, że wymienione powyżej praktyki negatywnie wpłynęły na zaufanie do przetwarzania w chmurze i dostawców usług przetwarzania w chmurze w Stanach Zjednoczonych; podkreśla zatem, że rozwój europejskich chmur obliczeniowych i rozwiązań informatycznych jest elementem istotnym dla wzrostu gospodarczego i zatrudnienia oraz zaufania do usług przetwarzania w chmurze i dostawców takich usług, a także dla zapewnienia wysokiego poziomu ochrony danych osobowych;

65. wzywa wszystkie organy publiczne w Unii, aby nie wykorzystywały usług przetwarzania w chmurze w przypadkach, w których zastosowanie mogą mieć przepisy inne niż unijne;

66. ponownie wyraża poważne zaniepokojenie w odniesieniu do obowiązku bezpośredniego ujawniania danych i informacji osobowych obywateli UE, które są przetwarzane w ramach umów o świadczenie usług w chmurze obliczeniowej, władzom państw trzecich przez dostawców usług w chmurze podlegających prawu państw trzecich lub wykorzystujących serwery znajdujące się na terenie tych państw, a także w odniesieniu do zdalnego dostępu do danych osobowych i informacji przetwarzanych przez organy ścigania i służby wywiadowcze państw trzecich;

67. głęboko ubolewa, że taki dostęp jest zazwyczaj osiągany za pomocą bezpośredniego egzekwowania przez organy państw trzecich z wykorzystaniem ich własnych przepisów, bez uciekania się do instrumentów międzynarodowych służących współpracy prawnej, takich jak porozumienia o wzajemnej pomocy prawnej lub inne formy współpracy sądowej;

68. wzywa Komisję i państwa członkowskie do zwiększenia tempa prac nad ustanowieniem Europejskiego Partnerstwa na rzecz Chmur Obliczeniowych z pełnym zaangażowaniem społeczeństwa obywatelskiego i środowiska technicznego, np. grupy zadaniowej ds. inżynierii internetowej (IETF), oraz uwzględnieniem aspektów ochrony danych;

69. wzywa Komisję, by podczas negocjacji porozumień międzynarodowych, które dotyczą przetwarzania danych osobowych, zwracała szczególną uwagę na zagrożenia i wyzwania, jakie niesie chmura obliczeniowa dla praw podstawowych, a zwłaszcza – ale nie wyłącznie – prawa do prywatności i ochrony danych osobowych zgodnie z art. 7 i 8 Karty praw podstawowych Unii Europejskiej; ponadto wzywa Komisję do zwrócenia uwagi na te przepisy obowiązujące w kraju partnera w negocjacjach, które dotyczą dostępu organów ścigania i agencji wywiadowczych do danych osobowych przetwarzanych w ramach usług w chmurze obliczeniowej, zwłaszcza wymagając, by udzielanie takiego dostępu miało miejsce jedynie w następstwie rzetelnego procesu sądowego i na mocy jednoznacznych podstaw prawnych, a także by określono szczegółowe warunki udzielania takiego dostępu, środki bezpieczeństwa stosowane w momencie przekazywania danych, prawa jednostek, a także przepisy dotyczące nadzoru i efektywnych środków naprawczych;

70. przypomina, że wszystkie przedsiębiorstwa świadczące usługi w UE muszą bez wyjątku przestrzegać prawa UE i że są odpowiedzialne za wszelkie naruszenia oraz podkreśla znaczenie funkcjonowania skutecznych, proporcjonalnych i odstraszających sankcji administracyjnych, które można nakładać na usługodawców świadczących usługi przetwarzania w chmurze, którzy nie spełniają unijnych norm ochrony danych osobowych;

71. wzywa Komisję i właściwe organy państw członkowskich do oceny stopnia, w jakim naruszono przepisy UE dotyczące prywatności i ochrony danych na skutek współpracy podmiotów prawnych w UE z tajnymi służbami lub na skutek zastosowania się do wydanych przez organy państw trzecich sądowych nakazów udostępnienia danych osobowych obywateli UE wbrew unijnemu prawodawstwu dotyczącemu ochrony danych osobowych;

72. wzywa przedsiębiorstwa świadczące nowe usługi z wykorzystaniem dużych zbiorów danych i dostarczające nowe aplikacje, takie jak „internet przedmiotów", do wprowadzenia środków ochrony danych już na etapie opracowywania w celu utrzymania wysokiego poziomu zaufania obywateli;

Transatlantyckie partnerstwo w dziedzinie handlu i inwestycji (TTIP)

73. przyjmuje do wiadomości, że UE i Stany Zjednoczone prowadzą negocjacje w sprawie transatlantyckiego partnerstwa w dziedzinie handlu i inwestycji, które ma istotne znaczenie strategiczne dla zapewnienia dalszego wzrostu gospodarczego;

74. zdecydowanie podkreśla, że biorąc pod uwagę znaczenie gospodarki cyfrowej w tej relacji i w odbudowie zaufania między UE a Stanami Zjednoczonymi, nie można być pewnym zgody Parlamentu Europejskiego na ostateczną umowę w sprawie TTIP, dopóki nie zostanie całkowicie wstrzymany nieograniczony nadzór na masową skalę oraz przechwytywanie komunikacji w instytucjach i przedstawicielstwach dyplomatycznych UE, a także dopóki nie zostanie znalezione odpowiednie rozwiązanie dotyczące praw obywateli UE do zachowania prywatności danych, w tym sądowych

i administracyjnych mechanizmów dochodzenia roszczeń; podkreśla, że Parlament może wydać zgodę na ostateczną umowę w sprawie TTIP, pod warunkiem że umowa będzie w pełni uwzględniać m.in. poszanowanie praw podstawowych uznanych w karcie UE oraz że ochrona prywatności osób w odniesieniu do przetwarzania i rozpowszechniania danych osobowych będzie nadal uregulowana art. XIV GATS; podkreśla, że unijnego prawodawstwa dotyczącego ochrony danych nie można uznać za „arbitralną lub nieuzasadnioną dyskryminację" w zastosowaniu art. XIV GATS;

Demokratyczny nadzór nad służbami wywiadowczymi

75. podkreśla, że chociaż nadzór nad działaniami służb wywiadowczych powinien opierać się zarówno na legitymacji demokratycznej (silnych ramach prawnych, upoważnieniu ex ante i weryfikacji ex post), jak i na odpowiednich zdolnościach technicznych i wiedzy fachowej, większości obecnych unijnych i amerykańskich organów nadzoru zdecydowanie brakuje ich obu, zwłaszcza zdolności technicznych;

76. podobnie jak w przypadku Echelonu, wzywa wszystkie parlamenty narodowe, które jeszcze tego nie uczyniły, do przyznania kompetencji prawnych w zakresie prowadzenia dochodzeń w ramach znaczącego nadzoru nad działaniami wywiadowczymi sprawowanego przez parlamentarzystów lub organy eksperckie; wzywa parlamenty narodowe do zapewnienia tego, aby takie komisje/organy nadzoru posiadały wystarczające zasoby, fachową wiedzę techniczną i środki prawne, w tym prawo do prowadzenia kontroli na miejscu, umożliwiające im sprawowanie skutecznej kontroli nad służbami wywiadowczymi;

77. wzywa do powołania grupy złożonej z posłów i ekspertów w celu zbadania, w sposób przejrzysty i we współpracy z parlamentami krajowymi, zaleceń służących nasileniu demokratycznej kontroli, w tym kontroli parlamentarnej nad służbami wywiadowczymi, oraz bardziej intensywnej współpracy w zakresie kontroli w UE, w szczególności w jej wymiarze transgranicznym; uważa, że grupa ta powinna rozważyć możliwość ustanowienia minimalnych europejskich norm lub wytycznych w zakresie nadzoru (ex ante i ex post) nad służbami wywiadowczymi w oparciu o obowiązujące sprawdzone wzorce postępowania i zalecenia organów międzynarodowych (ONZ, Rady Europy), w tym kwestię uznawania organów nadzorczych za osobę trzecią na podstawie „zasady osoby trzeciej" lub „zasady kontroli organu zastrzegającego", dotyczące sprawowania nadzoru nad wywiadem z państw obcych i pociągania go do odpowiedzialności, kryteria zwiększonej przejrzystości oparte na podstawie ogólnej zasady dostępu do informacji i tak zwanych „zasad z Tshwane" ([1]), a także zasady dotyczące ograniczenia czasu trwania i zakresu nadzoru, dbając o to, by były one proporcjonalne i ograniczone do celu nadzoru;

78. wzywa wspomnianą grupę do przygotowania sprawozdania na konferencję, jaką Parlament zorganizuje z początkiem 2015 r. wraz z krajowymi organami nadzoru, zarówno parlamentarnymi, jak i niezależnymi, oraz do wsparcia przygotowania tej konferencji;

79. wzywa państwa członkowskie do wykorzystania najlepszych praktyk, aby poprawić dostęp ich organów nadzoru do informacji na temat działań wywiadowczych (w tym informacji niejawnych i informacji pochodzących od innych służb) oraz ustanowienia uprawnień w zakresie przeprowadzania wizyt na miejscu, solidnego zbioru uprawnień w zakresie przesłuchań, odpowiednich zasobów i fachowej wiedzy technicznej, zdecydowanej niezależności od ich rządu oraz obowiązku sprawozdawczego wobec ich parlamentów;

80. wzywa państwa członkowskie do rozwoju współpracy między organami nadzoru, zwłaszcza w ramach europejskiej sieci ds. monitorowania krajowych służb wywiadowczych (ENNIR);

81. nalega na wysoką przedstawiciel/wiceprzewodniczącą, by regularnie informowała właściwe organy Parlamentu o działalności Centrum Analiz Wywiadowczych (IntCen) stanowiącego część Europejskiej Służby Działań Zewnętrznych, m.in. o pełnym przestrzeganiu praw podstawowych i mających zastosowanie przepisów UE o prywatności danych osobowych, umożliwiając lepszy nadzór Parlamentu nad zewnętrznym wymiarem polityk UE; wzywa Komisję i wysoką przedstawiciel/wiceprzewodniczącą do przedłożenia wniosku dotyczącego podstawy prawnej działalności IntCen, jeżeli przewidziane są jakiekolwiek operacje lub przyszłe uprawnienia w zakresie wywiadu lub możliwości samodzielnego gromadzenia danych, które mogłyby mieć wpływ na strategię UE w zakresie bezpieczeństwa wewnętrznego;

([1]) The Global Principles on National Security and the Right to Information (Globalne zasady w zakresie obrony narodowej i prawa do informacji), czerwiec 2013 r.

82. wzywa Komisję do przedstawienia do września 2014 r. wniosku dotyczącego unijnej procedury sprawdzającej w zakresie poświadczenia bezpieczeństwa wszystkich osób sprawujących urzędy w UE, ponieważ obecny system, który opiera się na poświadczaniu bezpieczeństwa przez państwa członkowskie obywatelstwa, przewiduje różne wymogi i różną długość procedur w systemach krajowych, co powoduje różne traktowanie posłów do Parlamentu i ich pracowników w zależności od ich obywatelstwa;

83. przypomina postanowienia porozumienia międzyinstytucjonalnego między Parlamentem Europejskim a Radą w sprawie przekazywania Parlamentowi Europejskiemu i przetwarzania przez Parlament posiadanych przez Radę informacji niejawnych dotyczących spraw innych niż z dziedziny wspólnej polityki zagranicznej i bezpieczeństwa, które należy wykorzystać do poprawy nadzoru na szczeblu UE;

Agencje UE

84. wzywa wspólny organ nadzorczy Europolu, aby wspólnie z krajowymi organami ds. ochrony danych przeprowadził do końca 2014 r. wspólną inspekcję w celu ustalenia, czy organy krajowe pozyskały informacje i dane osobowe wymieniane z Europolem w sposób zgodny z prawem, a zwłaszcza czy informacje lub dane zostały pierwotnie pozyskane przez służby wywiadowcze w UE czy w państwie trzecim oraz czy funkcjonują stosowne środki zapobiegające wykorzystywaniu i dalszemu rozpowszechnianiu takich informacji lub danych; uważa, że Europol nie powinien przetwarzać informacji ani danych uzyskanych z naruszeniem praw podstawowych, które są chronione na podstawie Karty praw podstawowych;

85. wzywa Europol, by w pełni skorzystał z uprawnienia do żądania od właściwych organów państw członkowskich, by wszczęły śledztwo w sprawie dużych ataków cybernetycznych i naruszeń informatycznych o potencjalnych skutkach transgranicznych; jest zdania, że należy wzmocnić mandat Europolu, tak by umożliwić mu wszczęcie własnego śledztwa w związku z podejrzeniem bezprawnego ataku na systemy sieciowe i informatyczne dwóch lub większej liczby państw członkowskich lub organów Unii ([1]); wzywa Komisję do przeprowadzenia przeglądu działań Europejskiego Centrum ds. Walki z Cyberprzestępczością oraz przedstawienia w razie konieczności wniosku dotyczącego kompleksowych ram służących zwiększeniu jego kompetencji;

Wolność wypowiedzi

86. wyraża głębokie zaniepokojenie wzrostem liczby zagrożeń dla wolności prasy i zniechęcaniem dziennikarzy do działania poprzez zastraszenie przez władze państwowe, co dotyczy zwłaszcza ochrony poufności źródeł dziennikarskich; ponownie występuje z postulatami wyrażonymi w swojej rezolucji z dnia 21 maja 2013 r. w sprawie Karty praw podstawowych UE: standardy określające wolność mediów w UE;

87. odnotowuje zatrzymanie Davida Mirandy i konfiskatę materiału znajdującego się w jego posiadaniu na podstawie załącznika 7 do ustawy o terroryzmie z 2000 r. (a także żądanie od „The Guardian" zniszczenia lub przekazania materiału) oraz wyraża obawę, że to może stanowić poważne naruszenie prawa do wolności wypowiedzi i wolności prasy uznanych w art. 10 EKPC i art. 11 karty UE oraz że można w takich przypadkach nadużywać prawa mającego na celu zwalczanie terroryzmu;

88. zwraca uwagę na trudną sytuację innych osób zgłaszających przypadki naruszenia i wspierających je osób, w tym dziennikarzy śledzących ich działalność; wzywa Komisję, by przeanalizowała, czy przyszły wniosek ustawodawczy wprowadzający skuteczny i kompleksowy europejski program ochrony osób zgłaszających przypadki naruszenia, jakiego Parlament domagał się już w rezolucji z 23 października 2013 r., powinien obejmować także inne dziedziny kompetencji Unii, ze szczególnym uwzględnieniem trudności, z jakimi wiąże się nagłaśnianie przypadków naruszeń w dziedzinie wywiadu; wzywa państwa członkowskie do gruntownego przeanalizowania możliwości zagwarantowania osobom zgłaszającym przypadki naruszenia ochrony międzynarodowej przed ściganiem;

([1]) Stanowisko Parlamentu Europejskiego z dnia 25 lutego 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Współpracy i Szkolenia w Dziedzinie Egzekwowania Prawa (Europol) (Teksty przyjęte, P7_TA(2014)0121).

89. wzywa państwa członkowskie, by dopilnowały, by ich prawo, zwłaszcza w dziedzinie bezpieczeństwa narodowego, przewidywało bezpieczne rozwiązanie alternatywne w stosunku do milczenia, dotyczące ujawniania lub zgłaszania nieprawidłowości, w tym korupcji, przestępstw, naruszeń przewidzianych prawem zobowiązań, pomyłek sądowych i nadużywania władzy, co jest także zgodne z przepisami zawartymi w rozmaitych instrumentach międzynarodowych (ONZ i Rady Europy) przeciwdziałających korupcji, zasadami ustanowionymi w rezolucji Zgromadzenia Parlamentarnego Rady Europy 1729 z 2010 r., zasadami z Tshwane itp.;

Bezpieczeństwo informatyczne w UE

90. wskazuje, że ostatnie zdarzenia wyraźnie świadczą o dużej podatności UE, a zwłaszcza instytucji UE, rządów krajowych i parlamentów narodowych, dużych przedsiębiorstw europejskich, europejskich infrastruktur i sieci informatycznych na zaawansowane ataki, w których wykorzystuje się złożone i złośliwe oprogramowanie; zauważa, że ataki te wymagają środków finansowych i zasobów ludzkich o takiej skali, że mogą mieć swoje źródło w podmiotach państwowych działających w imieniu rządów zagranicznych; w tym kontekście uważa przypadek złamania zabezpieczeń lub założenie podsłuchu w spółce telekomunikacyjnej Belgacom za niepokojący przykład ataku na zdolności informatyczne UE; podkreśla, że zwiększenie zdolności informatycznej UE i bezpieczeństwa w tej dziedzinie zmniejsza także podatność UE na poważne ataki cybernetyczne ze strony dużych organizacji przestępczych lub grup terrorystycznych;

91. jest zdania, że doniesienia o prowadzonym na masową skalę nadzorze, które rozpoczęły ten kryzys, można wykorzystać jako szansę wykazania przez Europę inicjatywy i utworzenia silnych i autonomicznych kluczowych zasobów informatycznych, co powinno być strategicznym priorytetem; podkreśla, że w celu odbudowy zaufania taki europejski potencjał informatyczny musi w jak największym stopniu opierać się na otwartych standardach oraz otwartym oprogramowaniu, a w miarę możliwości sprzęcie komputerowym, co umożliwi każdej zainteresowanej stronie przegląd całego łańcucha dostaw od projektu procesora do poziomu aplikacji w warunkach przejrzystości; wskazuje, że w celu przywrócenia konkurencyjności w strategicznym sektorze usług informatycznych potrzebny jest nowy ład cyfrowy oraz wspólne, zakrojone na szeroką skalę wysiłki instytucji UE, państw członkowskich, instytucji badawczych, przemysłu i społeczeństwa obywatelskiego; wzywa Komisję i państwa członkowskie do wykorzystania zamówień publicznych jako dźwigni w celu wsparcia potencjału tych zasobów w UE poprzez określenie standardów UE w zakresie bezpieczeństwa i prywatności jako zasadniczego wymogu w zamówieniach publicznych na towary i usługi informatyczne; dlatego nalega na Komisję, by dokonała przeglądu obecnej praktyki udzielania zamówień publicznych w odniesieniu do przetwarzania danych, żeby rozważyć ograniczenie procedur przetargowych do przedsiębiorstw certyfikowanych, a w miarę możliwości do przedsiębiorstw z UE, jeżeli w grę wchodzi bezpieczeństwo lub inne kluczowe interesy;

92. zdecydowanie potępia to, że służby wywiadowcze dążyły do obniżenia standardów bezpieczeństwa informatycznego i wstawienia luk typu backdoor w wielu różnych systemach informatycznych; zwraca się do Komisji o przedstawienie projektu przepisów mających na celu zakazanie stosowania luk typu backdoor przez organy ścigania; zaleca w związku z tym wykorzystanie otwartego oprogramowania we wszystkich środowiskach, w których istotne znaczenie ma bezpieczeństwo informatyczne;

93. wzywa wszystkie państwa członkowskie, Komisję, Radę i Radę Europejską do udzielenia jak najpełniejszego wsparcia, m.in. poprzez finansowanie w dziedzinie badań naukowych i rozwoju, na rzecz rozwoju europejskiego potencjału innowacyjnego i technologicznego w zakresie narzędzi, przedsiębiorstw i dostawców informatycznych (co dotyczy sprzętu komputerowego, oprogramowania, usług i sieci), także w celu zapewnienia bezpieczeństwa cybernetycznego oraz zdolności w zakresie szyfrowania i kryptografii; wzywa wszystkie odpowiedzialne instytucje i państwa członkowskie UE do inwestowania w lokalne i niezależne technologie UE oraz do intensywnego rozwijania i zwiększania zdolności wykrywania;

94. wzywa Komisję, organy normalizacyjne i Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, aby do grudnia 2014 r. opracowały minimalne normy w zakresie bezpieczeństwa i prywatności oraz wytyczne dotyczące systemów, sieci i usług informatycznych, w tym usług przetwarzania w chmurze, w celu lepszej ochrony danych osobowych obywateli UE oraz integralności wszystkich systemów informatycznych; uważa, że normy takie mogą stać się punktami odniesienia dla nowych standardów na poziomie globalnym oraz powinny zostać ustalone w ramach otwartego i demokratycznego procesu, który nie byłby prowadzony przez jedno państwo, jeden podmiot lub jedno przedsiębiorstwo wielonarodowe; jest zdania, że chociaż konieczne jest uwzględnienie zasadnych aspektów egzekwowania prawa i wywiadu w celu wsparcia walki z terroryzmem, nie powinny one powodować ogólnego umniejszenia niezawodności wszystkich systemów informatycznych; wyraża poparcie dla ostatnich decyzji grupy zadaniowej ds. inżynierii internetowej (IETF) dotyczących uwzględnienia rządów w modelu zagrożeń dla bezpieczeństwa w internecie;

95. wskazuje, że unijne oraz krajowe telekomunikacyjne organy regulacyjne, a w niektórych przypadkach także przedsiębiorstwa telekomunikacyjne, wyraźnie zaniedbały bezpieczeństwo informatyczne swoich użytkowników i klientów; wzywa Komisję do pełnego wykorzystania jej obecnych uprawnień na podstawie dyrektywy ramowej dotyczącej prywatności w łączności elektronicznej i telekomunikacji w celu zwiększenia ochrony poufności komunikacji poprzez przyjęcie środków zapewniających zgodność urządzeń końcowych z prawem użytkowników do kontroli i ochrony swoich danych osobowych oraz zapewnienia wysokiego poziomu bezpieczeństwa sieci i usług telekomunikacyjnych, w tym także poprzez określenie wymogu szyfrowania komunikatów od początku do końca w oparciu o aktualny stan techniki;

96. popiera europejską strategię bezpieczeństwa cybernetycznego, lecz uważa, że nie obejmuje ona wszystkich możliwych zagrożeń i należy rozszerzyć jej zakres o działania państwa podejmowane w złej wierze; podkreśla potrzebę pełniejszego bezpieczeństwa informatycznego i odporności systemów informatycznych;

97. wzywa Komisję, aby najpóźniej do stycznia 2015 r. przedstawiła plan działania na rzecz osiągnięcia większej niezależności UE w sektorze informatycznym, obejmujący spójniejsze podejście do zwiększenia europejskich technologicznych zdolności informatycznych (w tym w zakresie systemów informatycznych, urządzeń, usług, przetwarzania w chmurze, szyfrowania i anonimizacji) oraz do ochrony strategicznej infrastruktury informatycznej (w tym pod względem własności i podatności);

98. wzywa Komisję, aby w ramach następnego programu prac dotyczącego programu „Horyzont 2020" ukierunkowała większe zasoby na pobudzenie europejskich badań, rozwoju, innowacji i szkoleń w dziedzinie technologii informatycznych, zwłaszcza technologii i infrastruktury zwiększającej ochronę prywatności, kryptologii, bezpiecznego przetwarzania, rozwiązań w zakresie otwartego oprogramowania zabezpieczającego i innych usług społeczeństwa informacyjnego, a także by wspierała wewnętrzny rynek europejskiego oprogramowania, sprzętu informatycznego oraz szyfrowane sposoby komunikacji i infrastrukturę komunikacyjną, m.in. dzięki rozwijaniu kompleksowej strategii przemysłowej UE dla branży informatycznej; uważa, że małe i średnie przedsiębiorstwa odgrywają kluczową rolę w badaniach; podkreśla, że nie należy udzielać finansowania ze środków unijnych na projekty, których jedynym celem jest opracowanie narzędzi uzyskania bezprawnego dostępu do systemów informatycznych;

99. zwraca się do Komisji o określenie aktualnych obowiązków i rozważenie najpóźniej do grudnia 2014 r. konieczności rozszerzenia mandatu, poprawy koordynacji lub przyznania dodatkowych zasobów i zwiększenia zdolności technicznych Centrum ds. Walki z Cyberprzestępczością Europolu oraz innych unijnych ośrodków zajmujących się specjalistycznymi ekspertyzami, Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, CERT-UE i EIOD w celu umożliwienia im odegrania kluczowej roli w zabezpieczeniu unijnych systemów komunikacji, skuteczniejszego prowadzenia dochodzeń w sprawach poważnych naruszeń informatycznych w UE i zapobiegania takim naruszeniom oraz prowadzenia (lub pomocy państwom członkowskim i organom UE w prowadzeniu) dochodzeń technicznych na miejscu w sprawach poważnych naruszeń informatycznych; w szczególności wzywa Komisję, by rozważyła wzmocnienie roli ENISA w obronie systemów wewnętrznych instytucji UE oraz ustanowienie w ramach struktury ENISA właściwego reagowania na incydenty komputerowe (CERT) dla UE oraz jej państw członkowskich;

100. zwraca się do Komisji o ocenę potrzeby utworzenia akademii informatycznej UE, która zrzeszałaby najlepszych, niezależnych ekspertów europejskich i międzynarodowych we wszystkich powiązanych dziedzinach i której zadaniem byłoby udzielanie wszystkim odpowiednim instytucjom i organom UE porad naukowych dotyczących technologii informatycznych, w tym strategii związanych z bezpieczeństwem;

101. wzywa właściwe służby sekretariatu Parlamentu Europejskiego do przeprowadzenia pod kierownictwem przewodniczącego PE najpóźniej do czerwca 2015 r. (oraz przedstawienia sprawozdania okresowego najpóźniej do grudnia 2014 r.) gruntownego przeglądu i oceny niezawodności bezpieczeństwa informatycznego Parlamentu z naciskiem na: środki budżetowe, zasoby kadrowe, zdolności techniczne, organizację wewnętrzną i wszystkie odpowiednie elementy w celu zapewnienia wysokiego poziomu bezpieczeństwa systemów informatycznych Parlamentu; uważa, że ocena taka powinna co najmniej skutkować analizą informacji i zaleceniami dotyczącymi:

— konieczności regularnych, ścisłych i niezależnych kontroli bezpieczeństwa i testów penetracyjnych przeprowadzanych z pomocą wybranych zewnętrznych ekspertów w dziedzinie bezpieczeństwa z zapewnieniem przejrzystości i gwarancją ich niezależności od państw trzecich lub wszelkiego rodzaju interesów własnych;

— włączenia do procedur przetargowych dotyczących nowych systemów informatycznych szczegółowych wymogów w zakresie bezpieczeństwa/prywatności w systemach informatycznych, opartych na sprawdzonych wzorcach postępowania, w tym możliwości wprowadzenia wymogu otwartego oprogramowania jako warunku zakupu lub wymogu, aby w przetargach dotyczących obszarów szczególnie wrażliwych i związanych z bezpieczeństwem udział brały zaufane europejskie przedsiębiorstwa;

— wykazu przedsiębiorstw, które zawarły umowę z Parlamentem w dziedzinie informatyki i telekomunikacji, z uwzględnieniem wszelkich ujawnionych informacji o ich współpracy z agencjami wywiadowczymi (takich jak doniesienia o umowach zawieranych przez NSA z takim przedsiębiorstwem jak RSA, którego produkty Parlament wykorzystuje, aby chronić zdalny dostęp posłów do PE i pracowników PE do ich danych), w tym oceny możliwości świadczenia takich samych usług przez inne przedsiębiorstwa, najlepiej europejskie;

— rzetelności i odporności oprogramowania, zwłaszcza gotowego oprogramowania komercyjnego, stosowanego przez instytucje UE i ich systemy informatyczne, w odniesieniu do penetracji i naruszeń, których dopuszczają się organy ścigania i organy wywiadowcze UE lub państw trzecich, także z uwzględnieniem odpowiednich norm międzynarodowych, zasad dotyczących sprawdzonych wzorców postępowania w zakresie zarządzania ryzykiem i bezpieczeństwem oraz spełniania standardów bezpieczeństwa sieci i informacji w UE, również pod względem naruszeń zabezpieczeń;

— wykorzystania większej liczby systemów bazujących na otwartym oprogramowaniu;

— kroków i środków, jakie należy podjąć w związku z większym wykorzystaniem narzędzi mobilnych (np. smartfonów, tabletów, zarówno służbowych, jak i osobistych) i skutków wywieranych na bezpieczeństwo informatyczne systemu;

— bezpieczeństwa łączności między różnymi miejscami prac Parlamentu i systemów informatycznych wykorzystywanych w Parlamencie;

— wykorzystania i lokalizacji serwerów i centrów informatycznych na potrzeby systemów informatycznych Parlamentu oraz skutków dla bezpieczeństwa i integralności systemów;

— wprowadzenia w życie obowiązujących przepisów dotyczących naruszeń bezpieczeństwa i bezzwłocznego powiadamiania właściwych organów przez dostawców publicznie dostępnych sieci telekomunikacyjnych;

— wykorzystania możliwości przechowywania w chmurze przez Parlament, w tym rodzaju danych przechowywanych w chmurze, sposobu ochrony zawartości i dostępu do niej oraz lokalizacji serwerów chmury, wraz ze sprecyzowaniem mających zastosowanie prawnych ram ochrony danych i działalności wywiadowczej, jak również oceny, jakie są możliwości korzystania wyłącznie z serwerów chmury, które znajdują się na terytorium UE;

— planu umożliwiającego wykorzystanie większej liczby technologii kryptograficznych, w szczególności pełnego poświadczonego szyfrowania w przypadku wszystkich usług informatycznych i usług łączności, takich jak przetwarzanie w chmurze, poczta elektroniczna, komunikatory i telefonia;

— wykorzystania podpisu elektronicznego w poczcie elektronicznej;

— planu dotyczącego korzystania w przypadku wiadomości elektronicznych z domyślnego standardu szyfrowania, takiego jak GNU Privacy Guard, który jednocześnie umożliwia wykorzystanie podpisów cyfrowych;

— możliwości utworzenia w Parlamencie bezpiecznego komunikatora umożliwiającego bezpieczną komunikację, opartego na serwerze, do którego dociera wyłącznie zaszyfrowana treść;

102. wzywa instytucje i organy UE, a zwłaszcza Radę Europejską, Radę, Europejską Służbę Działań Zewnętrznych (w tym delegatury UE), Komisję, Trybunał Sprawiedliwości i Europejski Bank Centralny do tego, aby najpóźniej do czerwca 2015 r. (wraz z przedstawieniem sprawozdania okresowego najpóźniej do grudnia 2014 r.) wykonały podobne zadanie we współpracy z ENISA, Europolem i CERT; zachęca państwa członkowskie do przeprowadzenia podobnej oceny;

103. podkreśla, że jeśli chodzi o działania zewnętrzne UE, należy przeprowadzić oceny związanych z nimi potrzeb budżetowych i bezzwłocznie przedsięwziąć pierwsze środki w przypadku Europejskiej Służby Działań Zewnętrznych (ESDZ) oraz przydzielić odpowiednie fundusze w projekcie budżetu na 2015 r.;

104. jest zdania, że zakrojone na szeroką skalę systemy informatyczne wykorzystywane w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, takie jak system informacyjny Schengen II, wizowy system informacyjny, Eurodac, i ewentualne przyszłe systemy, takie jak EU-ESTA, powinny być opracowane i działać w sposób zapobiegający narażeniu danych na ryzyko na skutek żądań władz państw trzecich; zwraca się do eu-LISA o przedstawienie Parlamentowi sprawozdania na temat rzetelności funkcjonujących systemów do końca 2014 r.;

105. wzywa Komisję i ESDZ do podjęcia działania na szczeblu międzynarodowym, zwłaszcza wraz z ONZ, we współpracy z zainteresowanymi partnerami w celu realizacji unijnej strategii na rzecz demokratycznego zarządzania internetem, aby zapobiec niepotrzebnemu wpływowi poszczególnych podmiotów, przedsiębiorstw lub państw na działania ICANN i IANA poprzez zapewnienie odpowiedniej reprezentacji wszystkich zainteresowanych stron w tych organach, przy jednoczesnym unikaniu wspierania kontroli państwa czy cenzury lub „bałkanizacji" i fragmentaryzacji internetu;

106. wzywa UE, by objęła przewodnią rolę w przebudowie struktury internetu i zarządzania nim, by zaradzić zagrożeniom związanym z przepływami i przechowywaniem danych, w dążeniu do większej minimalizacji i przejrzystości danych oraz zmniejszenia skali centralnego masowego przechowywania danych surowych, a także do pełnego szyfrowania całości ruchu internetowego, od początku do końca, tak aby zapobiec obecnym zagrożeniom związanym z niepotrzebnym kierowaniem ruchu przez terytorium państw, które nie spełniają podstawowych standardów dotyczących praw podstawowych, ochrony danych i prywatności;

107. apeluje o promowanie:

— unijnych wyszukiwarek internetowych i unijnych serwisów społecznościowych jako cennego kroku w kierunku niezależności informatycznej UE;

— europejskich dostawców usług informatycznych;

— ogólnie szyfrowania komunikacji, w tym wiadomości e-mail i krótkich wiadomości tekstowych;

— kluczowych europejskich elementów informatycznych, na przykład rozwiązań w zakresie modelu klient–serwer–system operacyjny, stosowania standardów otwartego oprogramowania, rozwoju europejskich elementów służących do połączenia sieci, np. routerów;

108. wzywa Komisję do przedstawienia wniosku ustawodawczego w sprawie unijnego systemu trasowania (routing system), w tym przetwarzania informacji generowanych przez elementy infrastruktury teleinformatycznej (call detail records – CDR) na szczeblu UE, który będzie stanowił podstrukturę istniejącego Internetu i nie będzie wykraczał poza granice UE; zauważa, że wszystkie dane systemu trasowania oraz informacje CDR powinny być przetwarzane zgodnie z ramami prawnymi UE;

109. wzywa państwa członkowskie, aby we współpracy z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji, Centrum ds. Walki z Cyberprzestępczością Europolu, zespołami reagowania na incydenty komputerowe oraz krajowymi organami ds. ochrony danych i jednostkami ds. cyberprzestępczości rozwijały kulturę bezpieczeństwa i rozpoczęły kampanię edukacyjną i informacyjną w celu umożliwienia obywatelom podjęcia bardziej świadomej decyzji o tym, które dane osobowe udostępnić w internecie, oraz o sposobie ich lepszej ochrony, w tym dzięki szyfrowaniu i bezpiecznemu przetwarzaniu w chmurze, z pełnym wykorzystaniem platformy rozpowszechniania informacji użyteczności publicznej przewidzianej w dyrektywie w sprawie usługi powszechnej;

110. wzywa Komisję, aby do grudnia 2014 r. przedstawiła wnioski ustawodawcze mające na celu zachęcenie producentów oprogramowania i sprzętu komputerowego do wprowadzenia większego bezpieczeństwa i większej ochrony prywatności za pomocą uwzględnienia ochrony prywatności już w fazie projektowania i domyślnych opcji w ich produktach, w tym poprzez zastosowanie środków zniechęcających do niepotrzebnego i nieproporcjonalnego gromadzenia danych osobowych na masową skalę oraz wprowadzenie odpowiedzialności prawnej producentów za nienaprawione znane błędy, wadliwe bądź nie w pełni bezpieczne oprogramowanie lub wstawianie ukrytych luk typu backdoor umożliwiających nieautoryzowany dostęp do danych i ich przetwarzanie; w związku z powyższym wzywa Komisję, aby oceniła możliwość ustanowienia systemu certyfikowania lub walidacji dla sprzętu komputerowego IT obejmującego procedury testowania na szczeblu UE w celu zapewnienia integralności i bezpieczeństwa produktów;

Odbudowa zaufania

111. uważa, że oprócz potrzeby wprowadzenia zmian ustawodawczych śledztwo wykazało, iż Stany Zjednoczone muszą przywrócić zaufanie swoich partnerów z UE, ponieważ w grę wchodzą przede wszystkim działania agencji wywiadu USA;

112. wskazuje, że kryzys zaufania obejmuje:

— ducha współpracy w obrębie UE, ponieważ niektóre krajowe działania wywiadowcze mogą zagrażać osiągnięciu celów Unii;

— obywateli, którzy zdają sobie sprawę, że szpiegować ich mogą nie tylko państwa trzecie lub przedsiębiorstwa wielonarodowe, lecz również ich własny rząd;

— poszanowanie praw podstawowych, demokracji i rządów prawa, jak również wiarygodność gwarancji demokratycznych, sądowych i parlamentarnych oraz nadzór nad społeczeństwem cyfrowym;

Między UE a USA

113. przypomina o historycznym i strategicznym partnerstwie między państwami członkowskimi UE a USA, które opiera się na wspólnej wierze w demokrację, rządy prawa i prawa podstawowe;

114. uważa, że masowa inwigilacja obywateli i szpiegowanie przywódców politycznych przez USA poważnie zaszkodziły stosunkom między UE a USA i podważyły zaufanie do organizacji amerykańskich działających w UE; aspektem powodującym zaostrzenie problemu jest brak w amerykańskim prawie sądowych i administracyjnych środków umożliwiających dochodzenie roszczeń przez obywateli UE, szczególnie w przypadku działań w zakresie nadzoru prowadzonych w celach wywiadowczych;

115. przyznaje, że w świetle globalnych wyzwań, którym muszą sprostać UE i USA, partnerstwo transatlantyckie musi być w dalszym stopniu umacniane, a kontynuowanie transatlantyckiej współpracy w zwalczaniu terroryzmu na podstawie nowego zaufania opartego na prawdziwym wzajemnym poszanowaniu rządów prawa oraz odrzuceniu wszystkich niekontrolowanych praktyk prowadzonego na masową skalę nadzoru ma zasadnicze znaczenie; kładzie zatem nacisk na konieczność przedsięwzięcia przez USA wyraźnych środków, aby przywrócić zaufanie i ponownie podkreślić wspólne podstawowe wartości leżące u podstaw partnerstwa;

116. wyraża gotowość zaangażowania się w dialog z partnerami z USA, aby w bieżącej amerykańskiej debacie publicznej i kongresowej na temat reformy nadzoru i przeglądu nadzoru nad służbami wywiadowczymi poruszyć kwestię prawa do prywatności i innych praw przysługujących obywatelom UE, osobom zamieszkującym na terytorium UE lub innym osobom podlegającym ochronie na mocy prawa unijnego, zagwarantować równe prawa do informacji i ochrony prywatności w sądach amerykańskich, w tym środki dochodzenia roszczeń, dzięki np. przeglądowi ustawy o ochronie prywatności i ustawy o ochronie tajemnicy łączności elektronicznej oraz ratyfikacji pierwszego protokołu fakultatywnego do Międzynarodowego paktu praw obywatelskich i politycznych (MPPOiP), żeby nie przedłużać obecnej dyskryminacji;

117. nalega na podjęcie koniecznych reform i udzielenie Europejczykom skutecznych gwarancji, żeby stosowanie nadzoru i przetwarzania danych na potrzeby zagranicznych służb wywiadowczych miało proporcjonalny charakter, było ograniczone jasno określonymi warunkami oraz powiązane z racjonalnym podejrzeniem lub prawdopodobieństwem działalności terrorystycznej; podkreśla, że cel ten musi podlegać przejrzystej kontroli sądowej;

118. uważa, że potrzebne są jasne sygnały polityczne od naszych amerykańskich partnerów, które pokażą, że USA rozróżniają sojuszników od przeciwników;

119. wzywa Komisję i administrację USA do zajęcia się, w ramach bieżących negocjacji dotyczących umowy parasolowej między UE a USA w sprawie transferu danych w celu egzekwowania prawa, prawami obywateli UE do informacji i dochodzenia roszczeń, a także do zakończenia negocjacji do lata 2014 r., zgodnie z zobowiązaniem podjętym na posiedzeniu ministerialnym w obszarze sprawiedliwości i spraw wewnętrznych UE-USA z dnia 18 listopada 2013 r.

120. zachęca USA do przystąpienia do konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencja nr 108), na takiej samej zasadzie, na jakiej przystąpiły do Konwencji o cyberprzestępczości z 2001 r., co pozwoli umocnić wspólne podstawy prawne między sojusznikami transatlantyckimi;

121. wzywa instytucje unijne do wykorzystania możliwości ustanowienia wraz z USA kodeksu postępowania, który gwarantowałby powstrzymywanie się od szpiegowania instytucji i obiektów unijnych.

W ramach Unii Europejskiej

122. uważa również, że do utraty zaufania, również między państwami członkowskimi oraz między obywatelami UE a ich krajowymi władzami, doprowadziły zaangażowanie i działania państw członkowskich UE; stoi na stanowisku, że tylko pełna przejrzystość celów i środków nadzoru, debata publiczna, a wreszcie zmiana prawa, w tym zakończenie działań w zakresie masowego nadzoru oraz wzmocnienie systemu kontroli sądowej i parlamentarnej, pozwolą przywrócić utracone zaufanie; ponownie zwraca uwagę na trudności, z jakimi wiąże się opracowanie kompleksowych strategii politycznych UE w dziedzinie bezpieczeństwa w warunkach takich działań nadzoru na masową skalę, oraz podkreśla, że unijna zasada lojalnej współpracy wymaga, by państwa członkowskie powstrzymywały się od prowadzenia działań wywiadowczych na terytorium innych państw członkowskich;

123. zauważa, że niektóre państwa członkowskie prowadzą z władzami amerykańskimi dwustronne rozmowy na temat domniemanego szpiegostwa, a część z nich zawarła (Zjednoczone Królestwo) lub zamierza zawrzeć (Niemcy, Francja) tzw. umowy antyszpiegowskie; podkreśla, że te państwa członkowskie muszą w pełni respektować interesy i ramy prawne UE jako całości; uznaje takie umowy dwustronne za przeciwskuteczne i pozbawione znaczenia, jako że potrzebne jest europejskie podejście do tego problemu; wzywa Radę do informowania Parlamentu o prowadzonych przez państwa członkowskie pracach nad europejską wzajemną umową o nieszpiegowaniu;

124. uważa, że takie umowy nie mogą łamać traktatów unijnych, a zwłaszcza zasady lojalnej współpracy (na mocy art. 4 ust. 3 TUE), ani podważać polityki UE w ujęciu ogólnym, w szczególności polityki w obszarach rynku wewnętrznego, uczciwej konkurencji oraz rozwoju gospodarczego, przemysłowego i społecznego; decyduje o przeprowadzeniu przeglądu takich umów pod kątem ich zgodności z prawem europejskim i zastrzega sobie prawo do uruchomienia procedur przewidzianych w Traktatach w razie, gdyby takie porozumienia okazały się sprzeczne z zasadą spójności lub podstawowymi zasadami, na których opiera się Unia;

125. wzywa państwa członkowskie, by dołożyły wszelkich wysiłków w celu zapewnienia lepszej współpracy na rzecz gwarancji przeciw szpiegostwu, we współpracy z właściwymi organami i agencjami UE, na rzecz ochrony obywateli i instytucji UE, europejskich przedsiębiorstw, unijnego przemysłu, infrastruktury i sieci informatycznych oraz europejskich badań naukowych; uznaje, że aktywny udział zainteresowanych podmiotów z UE jest wstępnym warunkiem skutecznej wymiany informacji; zaznacza, że zagrożenia dla bezpieczeństwa nabrały bardziej międzynarodowego, rozproszonego i złożonego charakteru, co wymaga zwiększenia współpracy na szczeblu europejskim; jest zdania, że te okoliczności należy lepiej odzwierciedlić w traktach i dlatego wzywa do przeglądu traktatów, żeby wzmocnić pojęcie lojalnej współpracy między państwami członkowskimi i Unią w celu osiągnięcia obszaru bezpieczeństwa i zapobieżenia wzajemnemu szpiegostwu między państwami członkowskimi w Unii;

126. uważa, że absolutnie niezbędne jest wprowadzenie zabezpieczonych przed podsłuchami struktur komunikacji (poczta elektroniczna i telekomunikacja, w tym telefony stacjonarne i komórkowe) oraz zabezpieczonych przed podsłuchami sal konferencyjnych we wszystkich istotnych instytucjach UE oraz delegaturach UE; w związku z powyższym wzywa do ustanowienia kodowanego wewnętrznego systemu poczty elektronicznej w UE;

127. wzywa Radę i Komisję, by bez dalszej zwłoki udzieliły zgody na wniosek przyjęty przez Parlament Europejski w dniu 23 maja 2012 r., dotyczący rozporządzenia Parlamentu Europejskiego w sprawie szczegółowych przepisów regulujących wykonywanie przez Parlament Europejski uprawnień śledczych i zastępujący decyzję 95/167/WE, Euratom, EWWiS Parlamentu Europejskiego, Rady i Komisji, a przedstawiony na podstawie art. 226 TFUE; wzywa do przeglądu Traktatu w celu poszerzenia takich kompetencji śledczych, tak by objęły bez ograniczeń ani wyjątków wszystkie dziedziny kompetencji lub działania Unii, oraz ujęcia możliwości prowadzenia przesłuchań pod przysięgą;

Wymiar międzynarodowy

128. wzywa Komisję do przedstawienia, najpóźniej w styczniu 2015 r., strategii UE dotyczącej demokratycznego zarządzania internetem;

129. wzywa państwa członkowskie do udziału w 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności, aby „popierać przyjęcie dodatkowego protokołu do art. 17 Międzynarodowego paktu praw obywatelskich i politycznych na podstawie norm opracowanych i zatwierdzonych w ramach Międzynarodowej Konferencji oraz postanowień zawartych w ogólnym komentarzu nr 16 Komitetu Praw Człowieka do paktu w celu stworzenia mających ogólne zastosowanie standardów ochrony danych i ochrony prywatności zgodnie z rządami prawa"; zwraca się do państw członkowskich, aby w tym zadaniu uwzględniły apel o utworzenie międzynarodowej agencji ONZ, która będzie odpowiedzialna w szczególności za monitorowanie pojawiania się narzędzi nadzoru oraz regulowanie ich użycia i prowadzenie dochodzeń w sprawie ich użycia; zwraca się do wysokiej przedstawiciel/wiceprzewodniczącej Komisji oraz Europejskiej Służby Działań Zewnętrznych do przyjęcia aktywnego stanowiska w tej sprawie;

130. wzywa państwa członkowskie do opracowania w ramach ONZ spójnej i solidnej strategii, wspierając zwłaszcza rezolucję pt. „Prawo do prywatności w epoce cyfrowej" zainicjowaną przez Brazylię i Niemcy, a przyjętą przez Trzeci Komitet Zgromadzenia Ogólnego ONZ (Komitet Praw Człowieka) w dniu 27 listopada 2013 r., a także podejmując wszelkie inne działania na rzecz obrony na szczeblu międzynarodowym podstawowego prawa do prywatności i ochrony danych, przy jednoczesnym unikaniu jakichkolwiek ułatwień dla kontroli państwowej, cenzury czy fragmentacji internetu, w tym inicjatywę dotyczącą zawarcia traktatu międzynarodowego zakazującego działań nadzorczych na masową skalę oraz ustanowienia agencji sprawującej nadzór nad jego wykonywaniem;

Plan priorytetowy: „Habeas corpus w europejskiej przestrzeni cyfrowej – ochrona praw podstawowych w epoce cyfrowej"

131. postanawia przedłożyć obywatelom, instytucjom i państwom członkowskim UE wspomniane rekomendacje jako plan priorytetowy na następną kadencję; wzywa Komisję oraz inne instytucje, organy, biura i agencje UE, o których mowa w niniejszej rezolucji, zgodnie z art. 265 TFUE, do działania zgodnie z zaleceniami i wezwaniami zawartymi w niniejszej rezolucji;

132. postanawia ustanowić akt pt. „Habeas corpus w europejskiej przestrzeni cyfrowej – ochrona praw podstawowych w epoce cyfrowej" obejmujący następujących 8 działań, których realizację będzie nadzorował:

— Działanie 1: Przyjęcie pakietu w sprawie ochrony danych w 2014 r.;

— Działanie 2: Zawarcie umowy parasolowej między UE a USA gwarantującej podstawowe prawo obywateli do prywatności i ochrony danych oraz zapewniającej odpowiednie mechanizmy dochodzenia roszczeń dla obywateli UE, w tym w razie przekazywania danych z UE do USA w celach związanych z egzekwowaniem prawa;

— Działanie 3: Zawieszenie porozumienia w sprawie bezpiecznego transferu danych osobowych do czasu przeprowadzenia pełnego przeglądu i usunięcia bieżących luk prawnych, tak aby zagwarantować, że transfer danych osobowych w celach handlowych z Unii do USA odbywa się wyłącznie zgodnie z najwyższymi unijnymi normami;

— Działanie 4: Zawieszenie umowy w sprawie Programu śledzenia środków finansowych należących do terrorystów do czasu (i) zakończenia negocjacji w sprawie umowy parasolowej; (ii) dogłębnego zbadania sprawy na podstawie analizy UE oraz należytego uwzględnienia wszystkich obaw wyrażonych przez Parlament w swojej rezolucji z dnia 23 października 2013 r.;

— Działanie 5: Ocena wszelkich umów, mechanizmów czy wymiany z państwami trzecimi dotyczących danych osobowych, aby zapewnić, że prawa do prywatności oraz do ochrony danych osobowych nie są naruszane w związku z działaniami związanymi z nadzorem, oraz podjęcie niezbędnych działań wynikających z takiej oceny;

— Działanie 6: Ochrona rządów prawa i praw podstawowych obywateli UE (m.in. przed zagrożeniami dla wolności prasy), prawa opinii publicznej do otrzymywania bezstronnych informacji i korzystania z tajemnicy zawodowej (w tym w stosunkach między prawnikami a klientami), a także wzmocniona ochrona osób zgłaszających przypadki naruszenia;

— Działanie 7: Opracowanie europejskiej strategii na rzecz większej niezależności w dziedzinie IT („nowy ład cyfrowy" obejmujący przydział odpowiednich środków na szczeblu krajowym i unijnym) w celu nadania rozmachu przemysłowi informatycznemu i umożliwić przedsiębiorstwom europejskim wykorzystanie konkurencyjnego atutu UE, jakim jest ochrona prywatności;

— Działanie 8: Uczynienie z UE referencyjnego gracza w obszarze demokratycznego i neutralnego zarządzania internetem;

133. wzywa instytucje i państwa członkowskie UE, by propagowały akt „Habeas corpus w europejskiej przestrzeni cyfrowej – ochrona praw podstawowych w epoce cyfrowej"; zobowiązuje się do działania jako obrońca praw obywateli UE zgodnie z następującym harmonogramem monitorowania wdrażania:

— od kwietnia 2014 r. do marca 2015 r.: grupa monitorująca utworzona na podstawie zespołu śledczego przy komisji LIBE, odpowiedzialna za monitorowanie nowych doniesień wchodzących w zakres mandatu zespołu śledczego oraz za kontrolę nad wdrażaniem niniejszej rezolucji;

— od lipca 2014 r.: stały mechanizm kontroli transferu danych i sądowych środków dochodzenia roszczeń w ramach właściwej komisji;

— wiosna 2014 r.: formalne wezwanie Rady Europejskiej do włączenia zasady habeas corpus w europejskiej przestrzeni cyfrowej – ochrony praw podstawowych w epoce cyfrowej – do wytycznych, które mają zostać przyjęte na podstawie art. 68 TFUE;

— jesień 2014 r.: zobowiązanie, że zasada habeas corpus w europejskiej przestrzeni cyfrowej – ochrona praw podstawowych w epoce cyfrowej – i powiązane zalecenia będą służyły jako kluczowe kryteria zatwierdzenia następnego składu Komisji;

— 2014: konferencja europejskich ekspertów wysokiego szczebla z różnych dziedzin powiązanych z bezpieczeństwem informatycznym (w tym z dziedziny matematyki, kryptografii i technologii poprawiających ochronę prywatności), aby pomóc rozwijać europejską strategię informatyczną na następną kadencję;

— 2014-2015: regularne zwoływanie posiedzeń grupy ds. zaufania, danych i praw obywateli powołanej przez Parlament Europejski i Kongres USA, z udziałem innych zaangażowanych w sprawę parlamentów z państw trzecich, w tym z Brazylii;

— 2014-2015: konferencja z organami nadzoru nad służbami wywiadowczymi europejskich parlamentów narodowych;

o

o o

134. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie Europejskiej, Radzie, Komisji, parlamentom i rządom państw członkowskich, krajowym organom ds. ochrony danych, Europejskiemu Inspektorowi Ochrony Danych, eu-LISA, Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, Agencji Praw Podstawowych, Grupie Roboczej Art. 29, Radzie Europy, Kongresowi Stanów Zjednoczonych Ameryki, administracji amerykańskiej, prezydentowi, rządowi i parlamentowi Federacyjnej Republiki Brazylii oraz sekretarzowi generalnemu ONZ;

135. zobowiązuje Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych do omówienia na sesji plenarnej Parlamentu tej sprawy rok po przyjęciu niniejszej rezolucji; uważa za niezbędne przeprowadzenie kontroli stopnia wdrożenia wytycznych przyjętych przez Parlament oraz zbadanie przypadków, w których wytyczne te nie zostały wdrożone.