EVROPSKÝ PARLAMENT 2009 - 2014

Výbor pro občanské svobody, spravedlnost a vnitřní věci

2013/2188(INI)

8. 1. 2014

NÁVRH ZPRÁVY

o programu agentury NSA (Spojené státy) pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů EU a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí (2013/2188(INI))

Výbor pro občanské svobody, spravedlnost a vnitřní věci

Zpravodaj: Claude Moraes

PR_INI

OBSAH

Strana

NÁVRH USNESENÍ EVROPSKÉHO PARLAMENTU

o programu agentury NSA (Spojené státy) pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů EU a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí
(2013/2188(INI))

Evropský parlament,

– s ohledem na Smlouvu o Evropské unii (SEU), zejména na články 2, 3, 4, 5, 6, 7, 10, 11 a 21 této smlouvy,

– s ohledem na Smlouvu o fungování Evropské unie (SFEU), zejména na články 15, 16 a 218 a hlavu V této smlouvy,

– s ohledem na protokol č. 36 o přechodných ustanoveních a na článek 10 tohoto protokolu a na prohlášení č. 50 k tomuto protokolu,

– s ohledem Listinu základních práv Evropské unie, a zejména na její články 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 a 52,

– s ohledem na evropskou Úmluvu o lidských právech, zejména na její články 6, 8, 9, 10 a 13 a na protokoly k této úmluvě,

– s ohledem na Všeobecnou deklaraci lidských práv, zejména na její články 7, 8, 10, 11, 12 a 14[1],

– s ohledem na Mezinárodní pakt o občanských a politických právech, zejména na články 14, 17, 18 a 19 tohoto paktu,

– s ohledem na Úmluvu Rady Evropy o ochraně údajů (ETS č. 108) a na Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních údajů, o orgánech dozoru a toku údajů přes hranice ze dne 8. listopadu 2001 (ETS č. 181),

– s ohledem na Úmluvu Rady Evropy o kyberkriminalitě (ETS č. 185),

– s ohledem na zprávu, kterou dne 17. května 2010 předložil zvláštní zpravodaj OSN pro podporu a ochranu lidských práv a základních svobod v rámci boje proti terorismu[2],

– s ohledem na zprávu, kterou dne 17. dubna 2013 předložil zvláštní zpravodaj OSN pro podporu a ochranu práva na svobodu přesvědčení a projevu[3],

– s ohledem na pokyny o lidských právech a boji proti terorismu přijaté Výborem

[1] http://www.un.org/en/documents/udhr/
[2] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/134/10/PDF/N0848087.pdf?OpenElement
[3] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

ministrů Rady Evropy dne 11. července 2002,

– s ohledem na bruselskou deklaraci ze dne 1. října 2010 přijatou na 6. konferenci parlamentních výborů pro dohled nad zpravodajskými a bezpečnostními službami členských států Evropské unie,

– s ohledem na rezoluci Parlamentního shromáždění Rady Evropy č. 1954 (2013) o národní bezpečnosti a přístupu k informacím,

– s ohledem na zprávu o demokratické kontrole bezpečnostních služeb přijatou Benátskou komisí dne 11. června 2007[1], a očekávaje s velkým zájmem aktualizaci této zprávy, která by měla být předložena na jaře roku 2014,

– s ohledem na svědectví zástupců výborů pro dohled nad zpravodajskými službami Belgie, Nizozemska, Dánska a Norska,

– s ohledem na případy předložené francouzským[2], polským a britským[3] soudům a Evropskému soudu pro lidská práva[4] v souvislosti se systémy masového sledování,

– s ohledem na Úmluvu o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie vypracovanou Radou v souladu s článkem 34 Smlouvy o Evropské unii, a zejména na hlavu III této úmluvy[5],

– s ohledem na rozhodnutí Komise 520/2000 ze dne 26. července 2000 o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států,

– s ohledem na zprávy Komise o posouzení uplatňování zásad „bezpečného přístavu“ ze dne 13. února 2002 (SEK(2002)196) a ze dne 20. října 2004 (SEK(2004)1323),

– s ohledem na sdělení Komise ze dne 27. listopadu 2013 (COM(2013)847) o fungování bezpečného přístavu z hlediska občanů EU a společností usazených v EU a na sdělení Komise ze dne 27. listopadu 2013 o obnovení důvěry v tok údajů mezi EU a Spojenými státy (COM(2013)846),

– s ohledem na usnesení Evropského parlamentu ze dne 5. července 2000 o návrhu rozhodnutí Komise o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států, v němž vyjádřil názor, že úroveň ochrany v rámci tohoto systému by neměla být považována za odpovídající[6], a na stanoviska pracovní skupiny

[1] http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
[2] Mezinárodní federace lig lidských práv a Francouzská liga pro obranu lidských práv a občanů proti X; Soud prvního stupně v Paříži.
[3] Případy předložené Privacy International a Liberty vyšetřovacímu soudu.
[4] Společná žádost podle čl. 34 přeložená Big Brother Watch, Open Rights Group, English Pen Dr. Constanze Kurz (žadatelé) v. Spojené království (odpůrce).
[5] Úř. věst. C 197, 12.7.2000, s. 1.
[6] Úř. věst. C 121, 24.4.2001, s. 152.

zřízené podle článku 29, zejména stanovisko 4/2000 ze dne 16. května 2000[1],

– s ohledem na dohody mezi Spojenými státy americkými a Evropskou unií o používání a předávání jmenné evidence cestujících (dohoda o PNR) uzavřené v roce 2004, 2007[2] a 2012[3],

– s ohledem na společný přezkum provádění dohody mezi EU a Spojenými státy o zpracování a předávání jmenné evidence cestujících Ministerstvu vnitřní bezpečnosti Spojených států[4], společně se zprávou Komise určenou Evropskému parlamentu a Radě o společném přezkumu (COM(2013)844),

– s ohledem na stanovisko generálního advokáta Cruze Villalóna, který uvedl, že směrnice 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí je v plném rozsahu neslučitelná s čl. 52 odst. 1 Listiny základních práv Evropské unie a že článek 6 této směrnice je neslučitelný s článkem 7 a čl. 52 odst. 1 Listiny[5],

– s ohledem na rozhodnutí Rady 2010/412/EU ze dne 13. července 2010 o uzavření Dohody mezi Evropskou unií a Spojenými státy americkými o zpracovávání a předávání údajů o finančních transakcích z Evropské unie do Spojených států pro účely Programu sledování financování terorismu (TFTP)[6] a na doprovodná prohlášení Komise a Rady,

– s ohledem na Dohodu o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými[7],

– s ohledem na pokračující jednání o rámcové dohodě mezi EU a Spojenými státy americkými o ochraně osobních údajů při jejich předávání a zpracovávání pro účely prevence, vyšetřování, odhalování nebo stíhání trestných činů, včetně terorismu, v rámci policejní a justiční spolupráce v trestních věcech („zastřešující dohoda“),

– s ohledem na nařízení Rady (ES) č. 2271/96 ze dne 22. listopadu 1996 o ochraně proti účinkům právních předpisů přijatých určitou třetí zemí uplatňovaných mimo její území, jakož i proti účinkům opatření na nich založených nebo z nich vyplývajících[8],

– s ohledem na prohlášení prezidenta Brazilské federativní republiky při zahájení 68. zasedání Valného shromáždění OSN dne 24. září 2013 a na práci parlamentního výboru pro vyšetřování špionáže zřízeného brazilským Federálním senátem,

– s ohledem na zákon Spojených států o poskytování vhodných nástrojů pro stíhání

[1] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
[2] Úř. věst. L 204, 4.8.2007, s. 18.
[3] Úř. věst. L 215, 11.8.2012, s. 5.
[4] SEK(2013)630 ze dne 27.11.2013.
[5] Stanovisko generálního advokáta Cruze Villalóna ze dne 12. prosince 2013 ve věci C-293/12.
[6] Úř. věst. L 195, 27.7.2010, s. 3.
[7] Úř. věst. L 181, 19.7.2003, s. 34.
[8] Úř. věst. L 309, 29.11.1996, s. 1.

a bránění terorismu, který dne 26. října 2001 podepsal prezident George W. Bush,

– s ohledem na zákon o zahraničních zpravodajských službách (FISA) z roku 1978 a pozměňovací akt k tomuto zákonu z roku 2008,

– s ohledem na vládní příkaz č. 12333, který vydal v roce 1981 prezident USA a který byl pozměněn v roce 2008,

– s ohledem na legislativní návrhy, které v současné době projednává Kongres Spojených států, zejména na návrh zákona o naplňování práv a ukončení odposlechu, plošného shromažďování údajů a online sledování,

– s ohledem na přezkumy, které provedly Rada pro dohled nad respektováním soukromí a občanských svobod (Privacy and Civil Liberties Oversight Board), Národní bezpečnostní rada USA a skupina pro přezkum zpravodajských a komunikačních technologií zřízená prezidentem, zejména na zprávu „Svoboda a bezpečnost v měnícím se světě“, kterou uvedená skupina předložila dne 12. prosince 2013,

– s ohledem na rozhodnutí okresního soudu Spojených států pro Federální okres Columbia ve věci Klayman a další v. Obama a další, občanskoprávní řízení č. 13-0851, ze dne 16. prosince 2013,

– s ohledem na zprávu pracovní skupiny EU-USA pro ochranu údajů o závěrech této skupiny, kterou dne 27. listopadu 2013 předložili spolupředsedové[1] zastupující EU,

– s ohledem na svá usnesení ze dne 5. září 2001 a ze dne 7. listopadu 2002 o existenci globálního systému pro zachycování soukromé a obchodní komunikace (systém Echelon),

– s ohledem na své usnesení ze dne 21. května 2013 o Chartě EU: standardních podmínkách svobody sdělovacích prostředků v celé EU[2],

– s ohledem na své usnesení ze dne 4. července 2013 o programu sledování Národní bezpečnostní agentury USA, sledovacích subjektech v různých členských státech a jejich dopadu na soukromí občanů EU, v němž Evropský parlament pověřil Výbor pro občanské svobody, spravedlnost a vnitřní věci, aby provedl důkladné šetření této záležitosti[3],

– s ohledem na své usnesení ze dne 23. října 2013 o organizované trestné činnosti, korupci a praní peněz: doporučených krocích a iniciativách[4],

– s ohledem na své usnesení ze dne 23. října 2013 o pozastavení platnosti dohody TFTP v důsledku sledování prováděného americkou Agenturou pro národní bezpečnost[5],

[1] Dokument Rady č. 16987/13.
[2] Přijaté texty, P7_TA(2013)0203.
[3] Přijaté texty, P7_TA(2013)0322.
[4] Přijaté texty, P7_TA(2013)0444.
[5] Přijaté texty, P7_TA(2013)0449.

– s ohledem na své usnesení ze dne 10. prosince 2013 o uvolnění potenciálu cloud computingu v Evropě[1],

– s ohledem na interinstitucionální dohodu mezi Evropským parlamentem a Radou o předávání utajovaných informací v držení Rady, jež se týkají záležitostí mimo oblast společné zahraniční a bezpečnostní politiky, Evropskému parlamentu a jeho nakládání s nimi[2],

– s ohledem na přílohu VIII jednacího řádu,

– s ohledem na článek 48 jednacího řádu,

– s ohledem na zprávu Výboru pro občanské svobody, spravedlnost a vnitřní věci (A7-0000/2013),

Dopady masového sledování

A. vzhledem k tomu, že vazby mezi Evropou a Spojenými státy americkými vycházejí z ducha a zásad demokracie, svobody, práva a solidarity;

B. vzhledem k tomu, že vzájemná důvěra a porozumění jsou klíčovými faktory transatlantického dialogu;

C. vzhledem k tomu, že v září 2001 vstoupil svět do nové fáze, v jejímž důsledku většina vlád zařadila mezi své největší priority boj proti terorismu; vzhledem k tomu, že odhalení vycházející z dokumentů, které unikly díky Edwardu Snowdenovi, bývalému spolupracovníkovi NSA, donutila demokraticky zvolené představitele řešit problém rostoucích kapacit zpravodajských agentur v oblasti činností sledování a jejich dopadu na právní stát v demokratické společnosti;

D. vzhledem k odhalením, která od června 2013 vyvolala v EU značné obavy, pokud jde o:

- rozsah systémů sledování odhalených jak ve Spojených státech, tak v členských státech EU;
- vysoké riziko zneužití právních norem EU, základních práv a norem pro ochranu údajů;
- míru důvěry mezi transatlantickými partnery – EU a Spojenými státy;
- míru spolupráce a zapojení určitých členských států EU do programů Spojených států pro sledování nebo obdobných programů na vnitrostátní úrovni, kterou odhalily sdělovací prostředky;
- míru kontroly a účinného dohledu politických orgánů Spojených států a určitých členských států EU nad jejich zpravodajskými službami;
- možnost, aby byly operace masového sledování využívány pro jiné účely, než

[1] Přijaté texty, P7_TA(2013)0535.
[2] Úř. věst. C 353 E, 3.12.2013, s. 156–167.

je národní bezpečnost a důsledný boj proti terorismu, například k hospodářské a průmyslové špionáži či profilování z politických důvodů;

- úlohy a míru zapojení zpravodajských agentur a soukromých IT a telekomunikačních společností;
- stále nejasnější hranice mezi prosazováním práva a zpravodajskými činnostmi, což vede k tomu, že se s každým občanem zachází jako s podezřelým;
- ohrožení soukromí v digitální éře;

E. vzhledem k tomu, že orgány Spojených států, evropské orgány a instituce a vlády členských států a jejich vnitrostátní parlamenty musí v plném rozsahu prošetřit bezprecedentní rozsah odhalené špionáže;

F. vzhledem k tomu, že orgány Spojených států popřely některé z odhalených informací, ale většinu z nich nenapadly; vzhledem k tomu, že ve Spojených státech a v omezeném počtu členských států EU se rozvinula široká veřejná diskuze; vzhledem k tomu, že vlády EU příliš často mlčí a nezahajují odpovídající vyšetřování;

G. vzhledem k tomu, že povinností evropských orgánů a institucí je zajistit, aby byly právní předpisy EU plně uplatňovány v zájmu evropských občanů a aby nebyla právní síla Smluv EU narušována tím, že budou přijímány exteritoriální dopady norem a opatření třetích zemí, aniž by jim byla věnována pozornost;

Vývoj ve Spojených státech související s reformou zpravodajských služeb

H. vzhledem k tomu, že okresní soud Spojených států pro Federální okres Columbia ve svém rozhodnutí ze dne 16. prosince 2013 prohlásil, že hromadný sběr metadat ze strany NSA je v rozporu se čtvrtým dodatkem k ústavě Spojených států[1];

I. vzhledem k tomu, že obvodní soud Spojených států pro Východní obvod Michiganu ve svém rozhodnutí prohlásil, že čtvrtý dodatek vyžaduje přiměřenost všech pátrání, předchozí soudní příkazy pro veškeré odůvodněné vyšetřování, povolení, která budou založena na předem existujících pravděpodobných důvodech, specifický přístup k osobám, místům a věcem, a zprostředkování nestranného soudce mezi výkonnými úředníky donucovacích orgánu a občany[2];

J. vzhledem k tomu, že skupina jmenovaná prezidentem USA pro přezkum zpravodajských a komunikačních technologií ve své zprávě ze dne 12. prosince 2013 navrhuje prezidentovi Spojených států 45 doporučení; vzhledem k tomu, že doporučení zdůrazňují, že je třeba zároveň chránit národní bezpečnost a soukromí osob a občanské svobody; vzhledem k tomu, že v této souvislosti vyzývá vládu Spojených států, aby co nejrychleji ukončila hromadný sběr dat ze záznamů telefonických hovorů osob ve Spojených státech podle článku 215 zákona o poskytování vhodných nástrojů pro stíhání a bránění terorismu, přistoupila k důkladnému přezkumu právního rámce NSA a zpravodajských služeb Spojených

[1] Klayman a další v. Obama a další, občanskoprávní řízení č. 13-0851, ze dne 16. prosince 2013.
[2] ACLU v. NSA, č. 06-CV-10204, dne 17. srpna 2006.

států s cílem zajistit dodržování práva na soukromí, ukončila snahy o poškozování či vytváření zranitelného komerčního softwaru (backdoor a malware), zvýšila používání kódování, zejména v případě předávání údajů a nepodrývala úsilí o vytvoření norem kódování, vytvořila úřad advokáta veřejného zájmu, který by obhajoval soukromí a občanské svobody před soudem pro dohled nad zahraničními zpravodajskými službami, svěřila Radě pro dohled nad soukromím a občanskými svobodami pravomoc kontrolovat činnosti zpravodajských služeb pro účely zahraničního zpravodajství, nikoli jen pro účely boje proti terorismu, a přijímat stížnosti oznamovatelů, aby využívala smlouvy o vzájemné právní pomoci s cílem získat elektronickou komunikaci a nevyužívala sledování pro získávání průmyslového nebo obchodního tajemství;

K. vzhledem k tomu, že doporučení adresovaná prezidentovi Spojených států v souvislosti se zpravodajskými činnostmi, které se týkají osob, jež nejsou občany USA, podle článku 702 zákona FISA, uznávají zásadní význam respektování soukromí a lidské důstojnosti zakotveného v článku 12 Všeobecné deklarace lidských práv a v článku 17 Mezinárodního paktu o občanských a politických právech; vzhledem k tomu, že nedoporučují poskytování stejných práv a ochrany osobám, které nejsou občany USA, i občanům Spojených států;

Právní rámec

Základní práva

L. vzhledem k tomu, že zpráva pracovní skupiny EU-USA pro ochranu údajů o závěrech, kterou předložili spolupředsedové zastupující EU, uvádí přehled právní situace ve Spojených státech, ale nenapomohla dostatečnému zjištění skutečností týkajících se programů Spojených států pro sledování; vzhledem k tomu, že nebyla poskytnuta žádná informace o tzv. pracovní skupině „druhé úrovně“, v jejímž rámci členské státy vedou dvoustranná jednání s orgány Spojených států o otázkách souvisejících s národní bezpečností;

M. vzhledem k tomu, že základní práva, zejména svoboda projevu, tisku, myšlení, svědomí, náboženského vyznání a sdružování, právo na ochranu soukromí, ochrana údajů a právo na účinné opravné prostředky, presumpce neviny a právo na spravedlivý proces a nediskriminaci, zakotvená v Listině základních práv Evropské unie a v evropské Úmluvě o lidských právech jsou základními kameny demokracie;

Pravomoci Unie v oblasti bezpečnosti

N. vzhledem k tomu, že EU podle čl. 67 odst. 3 SFEU „usiluje o zajištění vysoké úrovně bezpečnosti“; vzhledem k tomu, že z ustanovení Smlouvy (zejména z čl. 4 odst. 2 SEU a článků 72 a 73 SFEU) vyplývá, že EU má určité pravomoci v záležitostech týkajících se společné bezpečnosti Unie; vzhledem k tomu, že EU využila své pravomoci v otázkách vnitřní bezpečnosti při rozhodování o určitých legislativních nástrojích a uzavírání mezinárodních dohod (PNR, TFTP), jejichž cílem je boj proti závažné trestné činnosti a terorismu, a při vypracovávání strategie vnitřní bezpečnosti a zřizování agentur pro činnost v této oblasti;

O. vzhledem k tomu, že pojmy „národní bezpečnost“, „vnitřní bezpečnost“, „vnitřní bezpečnost EU“ a „mezinárodní bezpečnost“ se překrývají; vzhledem k tomu, že Vídeňská úmluva o smluvním právu, zásada loajální spolupráce mezi členskými státy EU a zásada lidskoprávních právních předpisů o úzkém výkladu všech výjimek společně směřují k restriktivnímu výkladu pojmu „národní bezpečnost“ a vyžadují, aby členské státy nezasahovaly neoprávněně do pravomocí EU;

P. vzhledem k tomu, že podle evropské Úmluvy o lidských právech musí agentury členských států i soukromé subjekty působící v oblasti národní bezpečnosti dodržovat práva zakotvená v této úmluvě, ať už jde o práva jejich občanů nebo občanů jiných států; vzhledem k tomu, že stejná zásada platí pro spolupráci s orgány jiných států v oblasti národní bezpečnosti;

Exteritorialita

Q. vzhledem k tomu, že exteritoriální uplatňování zákonů, předpisů a jiných legislativních či výkonných nástrojů ze strany třetí země v situaci, která spadá do jurisdikce EU nebo jejích členských států, by mohlo mít dopad na vytvořený právní řád a právní stát, nebo by dokonce mohlo porušovat mezinárodní právní předpisy či právo EU, včetně práv fyzických či právnických osob, s přihlédnutím k rozsahu a deklarovanému či skutečnému cíli tohoto uplatňování; vzhledem k tomu, že za těchto výjimečných okolností je nezbytné podniknout na úrovni EU kroky k zajištění toho, aby byl v EU dodržován právní stát a práva fyzických a právnických osob, zejména odstranit či neutralizovat dopady příslušných právních předpisů cizích států, zamezit jim nebo je řešit jiným způsobem;

Mezinárodní předávání údajů

R. vzhledem k tomu, že předávání osobních údajů Spojeným státům orgány, institucemi a jinými subjekty EU nebo členskými státy za účelem prosazování práva při neexistenci odpovídajících záruk a ochran pro dodržování základních práv občanů EU, zejména práva na soukromí a ochranu osobních údajů, by vedlo k tomu, že orgán, instituce nebo jiný subjekt EU nebo členský stát by byl podle článku 340 SFEU nebo ustálené judikatury Soudního dvora EU[1] odpovědný za porušení právních předpisů EU, což zahrnuje jakékoli porušení základních práv zakotvených v Listině EU;

Předávání údajů subjektům usazeným ve Spojených státech na základě „zásad bezpečného přístavu“

S. vzhledem k tomu, že právní rámec Spojených států pro ochranu údajů nezajišťuje odpovídající úroveň ochrany pro občany EU;

T. vzhledem k tomu, že Komise, aby umožnila správcům údajů EU předávat osobní údaje subjektům ve Spojených státech, ve svém rozhodnutí 520/2000 prohlásila, že zásady „bezpečného přístavu“ a pokyny obsažené v „často kladených otázkách“ vydaných Ministerstvem obchodu Spojených států zajišťují odpovídající úroveň ochrany osobních údajů předávaných z Unie organizacím usazeným ve Spojených

[1] Viz zejména spojené věci C-6/90 a C-9/90, Francovich a další v. Itálie, rozsudek ze dne 28. května 1991.

státech, které se zavázaly dodržovat uvedené zásady

U. vzhledem k tomu, že ve svém usnesení ze dne 5. července 2000 Evropský parlament vyjádřil pochyby a obavy, pokud jde o odpovídající úroveň ochrany poskytované podle zásad „bezpečného přístavu“, a vyzval Komisi, aby rozhodnutí v přiměřené lhůtě přezkoumala s ohledem na zkušenosti a vývoj legislativního rámce;

V. vzhledem k tomu, že rozhodnutí Komise 520/2000 stanoví, že příslušné orgány v členských státech mohou s cílem chránit fyzické osoby v souvislosti se zpracováním jejich osobních údajů uplatnit své stávající pravomoci, aby zastavily toky údajů vůči organizaci, která sama osvědčila, že přistoupila k zásadám bezpečného přístavu, pokud je velmi pravděpodobné, že zásady jsou porušovány nebo pokud by pokračování v předávání údajů vyvolalo bezprostřední riziko vzniku vážné újmy subjektům údajů;

W. vzhledem k tomu, že rozhodnutí Komise 520/2000 uvádí, že pokud informace prokáží, že kterýkoli subjekt pověřený zajištěním toho, aby byly dodržovány uvedené zásady neplní účinně svou úlohu, uvědomí o tom Komise Ministerstvo obchodu Spojených států, a bude-li třeba, předloží návrh opatření s cílem zrušit toto rozhodnutí, pozastavit je nebo omezit jeho působnost;

X. vzhledem k tomu, že ve svých prvních dvou zprávách o provádění zásad bezpečného přípravu vypracovaných v roce 2002 a 2004 Komise uvedla několik nedostatků, pokud jde o řádné provádění těchto zásad, a vyslovila několik doporučení adresovaných orgánů Spojených států s cílem odstranit tyto nedostatky;

Y. vzhledem k tomu, že ve své třetí zprávě o provádění ze dne 27. listopadu 2013, devět let po předložení druhé zprávy, kdy žádný z nedostatků uvedených v této zprávě nebyl odstraněn, Komise poukázala na další rozsáhlé slabiny a závady, pokud jde o zásady bezpečného přístavu, a došla k závěru, že není možné pokračovat ve stávajícím uplatňování těchto zásad; vzhledem k tomu, že Komise zdůraznila, že rozsáhlý přístup zpravodajských služeb Spojených států k údajům předávaným Spojeným státům organizacemi osvědčujícími, že zachovávají zásady bezpečného přístavu, ve Spojených státech vyvolává další závažné otázky, pokud jde o kontinuitu ochrany údajů subjektů údajů z EU; vzhledem k tomu, že Komise formulovala 13 doporučení určených orgánům Spojených států a zavázala se do léta 2014 stanovit společně s orgány Spojených států nápravná opatření, která je třeba co nejrychleji uplatňovat, a vytvořit tak základ pro důkladný přezkum fungování zásad bezpečného přístavu;

Z. vzhledem k tomu, že ve dnech 28.–31. října 2013 se delegace Výboru pro občanské svobody, spravedlnost a vnitřní věci (výbor LIBE) setkala ve Washingtonu D.C.se zástupci Ministerstva obchodu Spojených států a Federální obchodní komise; vzhledem k tomu, že Ministerstvo obchodu uznalo, že některé organizace samy osvědčily, že se přihlásily k zásadám bezpečného přístavu, ale jednoznačně prokazují „neaktuální stav“, což znamená, že určitá společnost neplní požadavky bezpečného přístavu, ačkoli nadále přijímá osobní údaje z EU; vzhledem k tomu, že Federální obchodní komise připustila, že mechanismus bezpečného přístavu by měl být revidován s cílem zlepšit jej, zejména pokud jde o stížnosti a alternativní systémy řešení sporů;

AA. vzhledem k tomu, že dodržování zásad bezpečného přístavu může být omezeno pouze „v rozsahu nezbytném pro splnění požadavků bezpečnosti státu, veřejného zájmu nebo prosazování zákonů“; vzhledem k tomu, že jakožto výjimka ze základních práv musí být podobná výjimka vždy vykládána restriktivně a omezovat se na rozsah nezbytný a přiměřený v demokratické společnosti a právní předpisy musí jasně stanovovat podmínky a záruky, které toto omezení odůvodňují; vzhledem k tomu, že podobná výjimka by neměla být používána způsobem, který by podrýval ochranu zajištěnou právními předpisy EU o ochraně údajů a zásadami bezpečného přístavu;

AB. vzhledem k tomu, že masově využívaný přístup zpravodajských agentur Spojených států závažně narušil transatlantickou důvěru a měl negativní dopad na důvěru k organizacím Spojených států působícím v EU; vzhledem k tomu, že tato situace je dále umocněna nedostatkem soudních a správních opravných prostředků, které právní předpisy Spojených států poskytují občanům EU, a to zejména v případech sledování pro zpravodajské účely.

Předávání údajů do třetích zemí s odpovídající úrovní ochrany

AC. vzhledem k tomu, že podle odhalených informací a závěrů z vyšetřování prováděného výborem LIBE byly národní bezpečnostní agentury Nového Zélandu a Kanady ve velké míře zapojeny do masového sledování elektronické komunikace a aktivně spolupracovaly se Spojenými státy v rámci takzvaného programu „Five eyes“ a mohly si navzájem vyměňovat osobní údaje občanů EU předávané z EU;

AD. vzhledem k tomu, že rozhodnutí Komise 2013/65[1] a 2/2002 ze dne 20. prosince 2001[2] označuje úroveň ochrany zajišťovanou novozélandským a kanadským zákonem o ochraně osobních informací a elektronických dokumentech za odpovídající; vzhledem k tomu, že výše uvedená zjištění rovněž závažným způsobem poškozují důvěru v právní systémy těchto zemí, pokud jde o kontinuitu ochrany poskytovanou občanům EU; vzhledem k tomu, že Komise se tímto aspektem nezabývala;

Předávání údajů založená na smluvních doložkách a jiných nástrojích

AE. vzhledem k tomu, že směrnice 95/46/ES stanoví, že mezinárodní předávání údajů do třetí země se může uskutečňovat také prostřednictvím specifických nástrojů, pokud správce poskytne dostatečná ochranná opatření pro ochranu soukromí a základních práv a svobod osob, jakož i pro výkon odpovídajících práv;

AF. vzhledem k tomu, že tato ochranná opatření mohou zejména vyplývat z vhodných smluvních doložek;

AG. vzhledem k tomu, že směrnice 95/46/ES Komisi uděluje pravomoc rozhodnout, že některé standardní smluvní doložky představují dostatečná ochranná opatření vyžadovaná směrnicí, a vzhledem k tomu, že na tomto základě Komise přijala tři modely standardních smluvních doložek pro předávání údajů správcům a zpracovatelům (a dílčím zpracovatelům) ve třetích zemích;

[1] Úř. věst. L 28, 30.1.2013, s. 12.
[2] Úř. věst. L 2, 4.1.2002, s. 13.

AH. vzhledem k tomu, že podle rozhodnutí Komise, kterými se stanoví standardní smluvní doložky, mohou příslušné orgány v členských státech uplatnit své stávající pravomoci a zastavit toky údajů, pokud se zjistí, že právní předpisy platné pro dovozce údajů nebo dílčího zpracovatele jim ukládají povinnost odchýlit se od platných právních předpisů o ochraně údajů a tyto odchylky přesahují omezení nezbytná v demokratické společnosti v souladu s článkem 13 směrnice 95/46/ES, přičemž tyto požadavky mohou mít značný negativní dopad na záruky poskytované platnými právními předpisy o ochraně údajů a standardními smluvními doložkami, nebo pokud je velmi pravděpodobné, že standardní smluvní doložky v příloze nejsou nebo nebudou plněny a že další předávání údajů by vyvolalo bezprostřední riziko vzniku vážné újmy subjektům údajů;

AI. vzhledem k tomu, že vnitrostátní orgány pro ochranu údajů vypracovaly závazná podniková pravidla s cílem usnadnit mezinárodní předávání údajů v rámci nadnárodních korporací a poskytnout odpovídající záruky, pokud jde o ochranu soukromí a základních práv a svobod osob a pokud jde o výkon odpovídajících práv; vzhledem k tomu, že před jejich použitím musí být závazná podniková pravidla schválena příslušnými orgány členských států, poté co tyto orgány posoudí jejich soulad s právními předpisy Unie o ochraně údajů;

Předávání údajů založená na dohodě TFTP a dohodě PNR

AJ. vzhledem k tomu, že Evropský parlament ve svém usnesení ze dne 23. října 2013 vyjádřil závažné obavy ohledně odhalení týkajících se činností NSA, pokud jde o přímý přístup k údajům o finančních transakcích a souvisejícím údajům, což by mohlo představovat jednoznačné porušení dohody, zejména jejího článku 1;

AK. vzhledem k tomu, že Evropský parlament požádal Komisi, aby pozastavila platnost dohody a aby byly veškeré relevantní informace a dokumenty okamžitě k dispozici při všech jednáních Evropského parlamentu;

AL. vzhledem k tomu, že na základě tvrzení sdělovacích prostředků Komise rozhodla o zahájení konzultací se Spojenými státy podle článku 19 dohody TFTP; vzhledem k tomu, že dne 27. listopadu 2013 komisař Malmström informoval výbor LIBE, že po setkání se zástupci orgánů Spojených států a s ohledem na odpovědi, které orgány Spojených států poskytly v písemné podobě a v průběhu jednání, Komise rozhodla, že nebude pokračovat v konzultacích, neboť nebyly zjištěny skutečnosti prokazující, že by vláda Spojených států postupovala v rozporu s ustanoveními dohody, a vzhledem k tomu, že Spojené státy poskytly písemné ujištění, že nedošlo k žádnému přímému shromažďování údajů, které by bylo v rozporu s ustanoveními dohody TFTP;

AM. vzhledem k tomu, že v průběhu cesty delegace výboru LIBE do Washingtonu ve dnech 28.–31. října 2013 se delegace setkala se zástupci Ministerstva financí Spojených států; vzhledem k tomu, že Ministerstvo financí Spojených států konstatovalo, že od vstupu dohody TFTP v platnost nemělo přístup k údajům z databáze SWIFT v EU mimo rámec TFTP; vzhledem k tomu, že Ministerstvo financí Spojených států se odmítlo vyjádřit k tomu, zda měl jakýkoli jiný vládní orgán Spojených států nebo ministerstvo přístup k údajům z databáze SWIFT mimo rámec TFTP, nebo zda vláda USA věděla o činnostech NSA v oblasti masového sledování;

vzhledem k tomu, že dne 18. prosince 2013 pan Glenn Greenwald před vyšetřovacím výborem LIBE prohlásil, že NSA a GCHQ se zaměřovaly na sítě SWIFT;

AN. vzhledem k tomu, že belgické a nizozemské orgány pro ochranu údajů dne 13. listopadu 2013 rozhodly o společném vyšetřování bezpečnosti plateb uskutečněných prostřednictvím sítě SWIFT s cílem potvrdit, zda by třetí strany mohly získat neoprávněný nebo nelegální přístup k bankovním údajům evropských občanů[1];

AO. vzhledem k tomu, že podle společného přezkumu provádění dohody mezi EU a Spojenými státy o jmenné evidenci cestujících Ministerstvo vnitřní bezpečnosti Spojených států předalo údaje PNR agentuře NSA ve 23 případech, které byly jednotlivě posouzeny z hlediska boje proti terorismu, v souladu s konkrétními podmínkami dohody;

AP. vzhledem k tomu, že společný přezkum nezmiňuje skutečnost, že v případě zpracovávání osobních údajů pro zpravodajské účely nemají podle právních předpisů Spojených států osoby, které nejsou občany USA, žádnou soudní nebo správní cestu k ochraně svých práv, a že ústavní ochrana je poskytována pouze občanům USA; vzhledem k tomu, že tento nedostatek soudních nebo správních práv ruší účinky ochrany občanů EU podle stávající dohody PNR;

Předávání založená na Dohodě mezi EU a USA o vzájemné právní pomoci v trestních věcech

AQ. vzhledem k tomu, že Dohoda EU a USA o vzájemné právní pomoci v trestních věcech ze dne 6. června 2003[2] vstoupila v platnost dne 1. února 2010 a jejím účelem je usnadnit spolupráci mezi EU a USA zaměřenou na účinnější potírání trestné činnosti s náležitým ohledem na práva jednotlivců a zásady právního státu;

Rámcová dohoda o ochraně údajů v oblasti policejní a justiční spolupráce („zastřešující dohoda“)

AR. vzhledem k tomu, že účelem této všeobecné dohody je poskytnout právní rámec pro veškeré předávání osobních údajů mezi EU a USA výhradně za účelem prevence, vyšetřování, odhalování nebo stíhání trestných činů, včetně terorismu, v rámci policejní a justiční spolupráce v trestních věcech; vzhledem k tomu, že Rada tato jednání schválila dne 2. prosince 2010;

AS. vzhledem k tomu, že tato dohoda by měla stanovit jasné, přesné a právně závazné zásady pro zpracování údajů a měla by obzvláště občanům EU zajistit právo na přístup k jejich osobním údajům v USA, na jejich opravy a vymazání, na účinný mechanismus, který by občanům EU umožňoval správní a soudní nápravu, a na nezávislý dohled nad zpracováním údajů;

AT. vzhledem k tomu, že Komise ve svém prohlášení ze dne 27. listopadu 2013 uvedla, že výsledkem „zastřešující dohody“ by měla být vyšší úroveň ochrany občanů na obou

[1] 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
[2] Úř. věst. L 181, 19.7.2003, s. 25.

stranách Atlantiku a větší důvěra Evropanů ve výměnu údajů mezi EU a USA, neboť tato dohoda bude základem pro další rozvoj spolupráce a partnerství EU a USA na poli bezpečnosti;

AU. vzhledem k tomu, že jednání o dohodě nepokročila, neboť vláda USA vytrvale odmítá uznat práva občanů EU na správní a soudní nápravu a neboť existuje záměr udělit rozsáhlé výjimky ze zásad ochrany údajů zakotvených v dohodě, jako je zásada omezení účelu, uchovávání údajů nebo jejich další předání, ať už vnitrostátní či do zahraničí;

Reforma ochrany údajů

AV. vzhledem k tomu, že právě probíhá přezkum právního rámce EU pro ochranu údajů, jehož cílem je zavést ucelený, jednotný, moderní a stabilní systém pro veškeré činnosti související se zpracováním údajů v Unii; vzhledem k tomu, že v lednu 2012 předložila Komise soubor legislativních návrhů: obecné nařízení o ochraně údajů[1], které nahradí směrnici 95/46/ES a zavede jednotný právní předpis v celé EU, a směrnici[2], která poskytne harmonizovaný rámec pro všechny činnosti související se zpracováním údajů a prováděné orgány činnými v trestném řízení za účelem prosazování práva a zmenší stávající rozdíly mezi jednotlivými vnitrostátními právními předpisy;

AW. vzhledem k tomu, že dne 21. října 2013 přijal výbor LIBE své legislativní zprávy týkající se těchto dvou návrhů a rozhodnutí zahájit s Radou jednání, jejichž cílem by bylo schválení těchto právních nástrojů v průběhu tohoto legislativního období;

AX. vzhledem k tomu, že ačkoliv Evropská rada ve dnech 24. a 25. října 2013 vyzvala k včasnému přijetí pevného obecného rámce EU pro ochranu údajů s cílem posílit důvěru občanů a podniků v digitální ekonomiku, nepodařilo se jí zaujmout společný postoj k obecnému nařízení o ochraně údajů a k uvedené směrnici[3];

Bezpečnost výpočetní techniky a „cloud computing“

AY. vzhledem k tomu, že v usnesení ze dne 10. prosince[4] je zdůrazněn ekonomický potenciál, jaký má tzv. „cloud computing“ pro růst a zaměstnanost;

AZ. vzhledem k tomu, že úroveň ochrany údajů v prostředí souvisejícím s „cloud computing“ nesmí být nižší, než je úroveň ochrany požadovaná v jakémkoli jiném kontextu zpracování údajů; vzhledem k tomu, že právní předpisy Unie o ochraně údajů se již dnes plně vztahují na služby poskytované na základě „cloud computing“ a provozované v EU, neboť tyto předpisy jsou z technologického hlediska neutrální;

BA. vzhledem k tomu, že prostřednictvím hromadného sledování získávají zpravodajské služby přístup k osobním údajům občanů EU, které jsou ukládány na základě dohod, jež jsou založeny na „cloud computing“ a uzavřených a byly uzavřeny s hlavními

[1] KOM(2012) 11, 25.1.2012.
[2] KOM(2012) 10, 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

[4] AT-0353/2013 PE506.114V2.00.

poskytovateli služeb v oblasti „cloud computing“ z USA; vzhledem k tomu, že zpravodajské služby USA získaly přístup k osobním údajům uloženým na serverech, které se nacházejí na území EU, tak, že pronikly do vnitřních sítí společností Yahoo! a Google[1]; vzhledem k tomu, že takové kroky jsou porušením mezinárodních závazků; vzhledem k tomu, že není vyloučeno, že zpravodajské služby pronikly i k informacím, které si prostřednictvím služeb „cloud computing“ uložily veřejné orgány členských států či podniky a instituce;

Demokratický dohled nad zpravodajskými službami

BB. vzhledem k tomu, že zpravodajské služby plní důležitou úlohu při ochraně demokratické společnosti před vnitřními i vnějšími hrozbami; vzhledem k tomu, že za tímto účelem disponují zvláštními pravomocemi a schopnostmi; vzhledem k tomu, že tyto pravomoci mají být využívány s ohledem na zásady právního státu, neboť v opačném případě těmto službám hrozí, že ztratí svou legitimitu a oslabí demokratický charakter společnosti;

BC. vzhledem k tomu, že vysoká úroveň utajení, s níž je nutně spojena činnost zpravodajských služeb, aby se předešlo ohrožení probíhajících operací, odhalení typického způsobu práce nebo ohrožení životů agentů, znemožňuje úplnou transparentnost, veřejnou kontrolu a běžné demokratické či soudní přezkumy;

BD. vzhledem k tomu, že technologický rozvoj vedl k hlubší mezinárodní spolupráci zpravodajských služeb, v jejímž rámci dochází k výměně osobních údajů a často i ke stírání hranice mezi zpravodajskou činností a činností donucovacích orgánů;

BE. vzhledem k tomu, že většina stávajících vnitrostátních mechanismů a orgánů dohledu byla zavedena či přepracována v 90. letech 20. století a nemusela být nutně přizpůsobena rychlému technologickému rozvoji posledního desetiletí;

BF. vzhledem k tomu, že navzdory intenzivnější výměně informací mezi členskými státy EU a členskými státy a třetími zeměmi se demokratický dohled nad zpravodajskými službami stále provádí na vnitrostátních úrovních; vzhledem k sílícímu rozporu, který panuje mezi úrovní mezinárodní spolupráce na jedné straně a dohledovými možnostmi omezenými pouze na úroveň vnitrostátní na straně druhé a jenž vede k nedostatečné a neúčinné demokratické kontrole;

Hlavní zjištění

1. domnívá se, že informace, jež se nedávno objevily v tisku díky oznamovatelům a novinářům, a důkazy předložené odborníky během tohoto šetření přesvědčivě dokládají skutečnost, že existují rozsáhlé, složité a technologicky velmi vyspělé systémy, které zbudovaly zpravodajské služby USA a některých členských států s cílem v nebývalé míře shromažďovat, ukládat a analyzovat komunikační a lokalizační údaje a metadata všech občanů světa bez rozdílu a jakéhokoli podezření;

2. konkrétně poukazuje na zpravodajské programy americké bezpečnostní agentury

[1] The Washington Post , 31. října 2013.

NSA, které umožňují hromadné sledování občanů EU na základě přímého přístupu do centrálních serverů velkých internetových společností USA (program *PRISM*), analýzy obsahu a metadat (program *Xkeyscore*), obcházení internetového šifrování (*BULLRUN*) a proniknutí do počítačových a telefonních sítí, k lokalizačním údajům a do systémů zpravodajské agentury Spojeného království GCHQ (*UK Government Communications Headquarters*), k jejímu základnímu sledování (program *Tempora*) a do jejího dešifrovacího programu (*Egdehill*); domnívá se, že je pravděpodobné, že i v jiných zemích EU existují programy obdobného charakteru, byť menšího rozsahu, např. v rámci zpravodajských služeb ve Francii (Direction générale de la sécurité extérieure, DGSE), v Německu (Bundesnachrichtendiens, BND) a ve Švédsku (Försvarets radioanstalt, FRA);

3. bere na vědomí fakt, že britské zpravodajské služby GCHQ se údajně nabouraly „hacking“ nebo neoprávněně pronikly do systémů společnosti Belgacom; připomíná, že společnost Belgacom uvedla, že nemůže potvrdit, zda toto proniknutí do systémů bylo namířeno proti orgánům a institucím EU nebo zda na ně mělo dopad, a že použitý škodlivý software je mimořádně složitý a jeho rozvoj a použití vyžaduje rozsáhlé finanční i lidské zdroje, kterými soukromé subjekty nebo „hackeři“ nedisponují;

4. konstatuje, že byla značně otřesena důvěra: důvěra mezi oběma transatlantickými partnery, důvěra mezi členskými státy EU, důvěra mezi občany a jejich příslušnými vládami, důvěra v dodržování zásad právního státu a důvěra v zabezpečení služeb IT; domnívá se, že k obnovení důvěry ve všech těchto oblastech je nutné okamžitě vypracovat komplexní plán;

5. konstatuje, že některé vlády tvrdí, že tyto programy hromadného sledování jsou nezbytné k boji proti terorismu; boj s terorismem upřímně podporuje, ale je pevně přesvědčen o tom, že tento boj sám o sobě nemůže být nikdy důvodem k použití necílených, tajných a někdy dokonce protizákonných programů hromadného sledování; znepokojuje jej proto otázka, zda jsou tyto programy zákonné, nezbytné a přiměřené;

6. považuje za velmi diskutabilní, že by shromažďování údajů prováděné v takovém měřítku bylo prováděno pouze za účelem boje proti terorismu, neboť se jedná o shromažďování všech možných druhů údajů o všech občanech; poukazuje tudíž na to, že možná existují jiné mocenské důvody související s použitím moci, jako je politická a hospodářská špionáž;

7. vyslovuje pochybnosti o tom, zda jsou masové hospodářské špionáže některých členských států slučitelné s právními předpisy z oblasti vnitřního trhu EU a hospodářské soutěže, které jsou zakotveny v hlavách I a VII Smlouvy o fungování Evropské unie; vyzdvihuje zásadu upřímné spolupráce, která je definována v čl. 4 odst. 3 Smlouvy o Evropské unii, a zásadu, podle níž se členské státy mají „zdržet veškerých opatření, která by mohla ohrozit dosažení unijních cílů“;

8. poukazuje na to, že mezinárodní smlouvy, právní předpisy EU a USA ani vnitrostátní mechanismy dohledu nezajistily systém brzd a protiváh, který je nutný pro demokratickou kontrolu;

9. co nejdůrazněji odsuzuje rozsáhlé, systematické a paušální shromažďování osobních údajů nevinných osob, mezi nimiž jsou často důvěrné soukromé informace; zdůrazňuje, že systémy hromadného sledování zpravodajskými službami všech osob bez rozlišení představují vážné porušení základních práv občanů; podtrhuje, že soukromí není luxusním právem, ale základním kamenem svobodné a demokratické společnosti; navíc poukazuje na to, že hromadné sledování může mít případně nepříznivý dopad na svobodu tisku, myšlení a projevu a skrývá i značný potenciál pro zneužití shromážděných informací proti politickým protivníkům; podtrhuje, že k těmto činnostem hromadného sledování využívají zpravodajské služby zřejmě i nezákonné postupy a že tyto činnosti vzbuzují pochybnosti ohledně extrateritoriality vnitrostátních zákonů;

10. považuje programy sledování za další krok směrem k zavedení úplného ochranného státu, v němž se mění model trestního práva zavedený v demokratických společnostech, místo něhož je prosazována kombinace vymáhání práva a zpravodajských činností s nejasnými právními nástroji ochrany, což často není v souladu s demokratickým systémem brzd a protiváh a se základními právy, zejména s presumpcí neviny; v tomto ohledu připomíná rozhodnutí německého spolkového ústavního soudu[1] o zákazu preventivních policejních zátahových akcí („präventive Rasterfahndung“), pokud neexistuje důkaz o konkrétním ohrožení jiných vysoce významných, zákonem zaručených práv, při čemž stav obecného ohrožení nebo mezinárodního napětí není dostatečným zdůvodněním pro taková opatření;

11. je pevně přesvědčen o tom, že tajné právní předpisy, smlouvy a soudy porušují zásady právního státu; poukazuje na to, že žádné rozhodnutí soudu a správního orgánu státu, jenž není členem EU, které přímo či nepřímo povoluje sledování podobné tomu, jež přezkoumává toto šetření, nesmí být automaticky uznáno či provedeno, ale na tato jednotlivá rozhodnutí musí být uplatněny náležité vnitrostátní postupy pro vzájemné uznávání a právní pomoc, včetně pravidel stanovených v dvoustranných dohodách;

12. konstatuje, že výše uvedené obavy dále zesiluje rychlý technologický a společenský rozvoj; domnívá se, že se jedná o problém nebývalého rozsahu, neboť internet a mobilní zařízení jsou v moderním každodenním životě na každém kroku („všudypřítomná výpočetní technika“) a podnikatelský model většiny internetových společností je založen na zpracovávání osobních údajů všeho druhu, což ohrožuje integritu jedince;

13. za zcela jasné považuje zjištění zdůrazněné i technickými odborníky, kteří vypovídali v rámci tohoto šetření, podle něhož ve stávající fázi technologického vývoje nelze veřejným orgánům a institucím EU ani občanům zaručit, že bezpečnost jejich výpočetní techniky či soukromí je možné uchránit před neoprávněným vniknutím dobře vybavených třetích zemí či zpravodajských agentur EU („neexistuje 100% bezpečnost IT“); konstatuje, že tuto alarmující situaci lze zvrátit pouze tehdy, pokud Evropané budou ochotni věnovat dostatečné zdroje – jak lidské, tak i finanční – na ochranu nezávislosti a soběstačnosti Evropy;

14. důrazně odmítá tvrzení, že tyto otázky jsou čistě věcí národní bezpečnosti a že jsou

[1] Č. 1 BvR 518/02 ze dne 4. dubna 2006.

tedy výhradně v kompetenci členských států; připomíná nedávné rozhodnutí Soudního dvora, v němž se uvádí: „Ačkoli je přijetí opatření k zajištění vnitřní i vnější bezpečnosti státu věcí členských států, nemůže pouhá skutečnost, že se rozhodnutí týká bezpečnosti státu, vést k tomu, že se nepoužije unijní právo.“[1]; dále připomíná, že v sázce je jak ochrana soukromí všech občanů EU, tak i bezpečnost a spolehlivost všech komunikačních sítí EU; domnívá se proto, že diskuse a opatření na úrovni EU nejsou pouze legitimní, ale jsou rovněž otázkou nezávislosti a suverenity EU;

15. je potěšen skutečností, že v různých částech světa probíhají na téma tohoto šetření různé diskuse, šetření a přezkumy; poukazuje na celosvětovou reformu vládního sledování (Global Government Surveillance Reform), pod níž se podepsaly čelní světové společnosti z oblasti technologií a jež vyzývá k rozsáhlým změnám v právních předpisech upravujících vnitrostátní sledování, a to i k mezinárodnímu zákazu hromadného shromažďování údajů, s cíle pomoci zachovat důvěru veřejnosti v internet; s velkým zájmem bere na vědomí doporučení, jež nedávno zveřejnila skupina jmenovaná prezidentem USA za účelem přezkumu zpravodajských a komunikačních technologií; naléhavě vyzývá vlády, aby vzaly tyto výzvy a tato doporučení plně na vědomí a přepracovaly své vnitrostátní rámce upravující činnost zpravodajských služeb, aby tak mohly zavést vhodná ochranná opatření a náležitý dohled;

16. oceňuje instituce a odborníky, kteří přispěli k tomuto šetření; lituje skutečnosti, že orgány některých členských států odmítly spolupráci na šetření, které Evropský parlament vede jménem občanů; vítá otevřenost některých členů Kongresu a národních parlamentů;

17. je si vědom toho, že v tak omezeném časovém období bylo od července 2013 možné pouze předběžně prošetřit všechny dotčené otázky; bere na vědomí jak rozsah zjištění, tak i skutečnost, že dochází ke stále novým odhalením; zaujímá proto prozíravý postoj, jehož součástí je záměr předložit soubor konkrétních návrhů a vypracovat mechanismus pro návazná opatření v příštím volebním období, čímž se zajistí, že tato zjištění zůstanou důležitým tématem politického programu EU;

18. má v úmyslu požadovat, aby Evropská komise, jež má být jmenována po volbách v květnu 2014, přijala významné politické závazky, jejichž cílem bude uplatňovat návrhy a doporučení vyplývající z tohoto šetření; očekává, že kandidáti na příští členy Komise účastnící se nadcházejících parlamentních slyšení přijmou náležité závazky;

Doporučení

19. vyzývá orgány USA a členské státy EU, aby zakázaly paušální hromadné sledování a masové zpracovávání osobních údajů;

20. vyzývá určité členské státy EU, včetně Spojeného království, Německa, Francie, Švédska a Nizozemska, aby v potřebných oblastech zrevidovaly své vnitrostátní právní předpisy a postupy týkající se činnosti zpravodajských služeb, a zajistily tak jejich soulad s normami vyplývajícími z Evropské úmluvy o lidských právech (EÚLP)

[1] Č. 1 BvR 518/02 ze dne 4. dubna 2006.

a s jejich závazky v oblasti základních práv, pokud jde o ochranu údajů a soukromí a presumpci neviny; s ohledem na řadu informací o hromadném sledování ve Spojeném království, jež přinesly sdělovací prostředky, by zejména rád zdůraznil, že stávající právní rámec, který je daný složitým spolupůsobením tří samostatných právních předpisů: zákonem o lidských právech (1998), zákonem o zpravodajských službách (1994) a zákonem o regulaci vyšetřovacích pravomocí (2000), je třeba přepracovat;

21. vyzývá členské státy, aby nepřijímaly z třetích zemí údaje, které byly shromážděny nezákonným způsobem, a nepovolovaly na svých územích sledování prováděné vládami či agenturami třetích zemí, které je v rozporu s vnitrostátním právem dané země nebo neodpovídá právním zárukám stanoveným mezinárodními nástroji či nástroji EU, mimo jiné i ochraně lidských práv zakotvené v SEU, v EÚLP a v Listině základních práv EU;

22. vyzývá členské státy, aby okamžitě začaly plnit svou pozitivní povinnost danou Evropskou úmluvou o lidských právech, a to povinnost chránit své občany před sledováním ze strany třetích zemí, jež by bylo v rozporu s požadavky těchto členských států, a to i před sledováním prováděným za účelem zajištění národní bezpečnosti, a zaručit, že nedojde k oslabení právního státu extrateritoriálním použitím práva třetí země;

23. vyzývá generálního tajemníka Rady Evropy, aby zahájil postup na základě článku 52, podle něhož „každá vysoká smluvní strana na žádost generálního tajemníka Rady Evropy vysvětlí způsob, jakým její vnitřní právní předpisy zajišťují účinné uplatňování všech ustanovení úmluvy“;

24. vyzývá členské státy, aby neprodleně přijaly náležitá opatření, včetně soudních řízení, je-li programy hromadného sledování narušena jejich suverenita, a tedy porušeno obecné mezinárodní právo veřejné; dále vyzývá členské státy EU, aby uplatnily všechna dostupná mezinárodní opatření k ochraně základních práv občanů EU, zejména zahájením postupu pro podávání mezistátních stížností na základě článku 41 Mezinárodního paktu o občanských a politických právech;

25. vyzývá USA, aby neprodleně přezkoumaly své právní předpisy s cílem zajistit jejich soulad s mezinárodním právem, uznaly právo na soukromí a další práva občanů EU, zajistily občanům EU možnost soudní nápravy a podepsaly dodatkový protokol, který umožňuje předkládání stížností jednotlivci na základě Mezinárodního paktu o občanských a politických právech;

26. rozhodně nesouhlasí s uzavřením jakéhokoli dodatkového protokolu či pokynu k Úmluvě Rady Evropy o kyberkriminalitě (budapešťská úmluva), který by se týkal přeshraničního přístupu k uloženým počítačových datům a mohl by zpravodajským službám umožňovat legitimní přístup k údajům uloženým na území jiné jurisdikce, aniž by musely mít povolení a musely uplatnit stávající nástroje pro vzájemnou právní pomoc, neboť výsledkem by mohl být neomezený dálkový přístup orgánů pro vymáhání práva k serverům a počítačovým systémům umístěným v jiných jurisdikcích, což by bylo v rozporu s úmluvou Rady Evropy č. 108;

27. vyzývá Komisi, aby do července 2014 posoudila použitelnost nařízení ES č. 2271/96

na případy rozporů mezi právními předpisy v souvislosti s předáváním osobních údajů;

Mezinárodní předávání údajů

Právní rámec USA pro ochranu údajů a nástroj USA „bezpečný přístav“

28. konstatuje, že společnosti, které jsou podle zpráv sdělovacích prostředků zapojeny do rozsáhlého hromadného sledování údajů o občanech EU americkou zpravodajskou agenturou NSA, jsou společnosti, které se přihlásily k programu „bezpečný přístav“, a že „bezpečný přístav“ je právní nástroj využívaný k předávání osobních údajů z EU do USA (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); vyjadřuje znepokojení nad skutečností, že tyto společnosti připustily, že informace a sdělení, jež si jejich datová centra předávají, nešifrují, čímž zpravodajským službám umožňují jejich zachycení[1];

29. domnívá se, že masově využívaný přístup zpravodajských služeb USA k osobním údajům v EU zpracovávaným pomocí nástroje „bezpečný přístav“ nesplňuje sám o sobě kritéria pro získání výjimky z důvodu „národní bezpečnosti“;

30. je toho názoru, že zásady nástroje „bezpečný přístav“ neposkytují za stávajících okolností dostatečnou ochranu občanům EU, a proto by tato předávání měla probíhat na základě jiných nástrojů, například smluvních doložek nebo závazných podnikových pravidel, která stanoví konkrétní záruky a mechanismy ochrany;

31. vyzývá Komisi, aby vypracovala opatření, na jejichž základě bude okamžitě pozastavena platnost jejího rozhodnutí 520/2000 o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států;

32. vyzývá oprávněné orgány členských států, jmenovitě úřady pro ochranu údajů, aby využily svých stávajících pravomocí k okamžitému zastavení toků údajů směrem ke každému subjektu, který se přihlásil k dodržování zásad programu USA „bezpečný přístav“, a požadovaly, aby předávání takových údajů probíhalo na základě jiných nástrojů, pokud tyto nástroje budou poskytovat nezbytné záruky a mechanismy ochrany v souvislosti s ochranou soukromí, základními právy a svobodou jednotlivců;

33. vyzývá Komisi, aby s ohledem na rozdíly projevující se mezi právními systémy EU a USA pro ochranu osobních údajů předložila do června 2014 komplexní posouzení rámce USA pro ochranu soukromí, v němž budou zahrnuta obchodní a zpravodajská činnost i vymáhání práva;

Předávání do dalších třetích zemí s rozhodnutím o přiměřenosti

34. připomíná, že směrnice 95/46/ES stanoví, že k předávání osobních údajů do třetí země smí dojít, aniž by tím bylo dotčeno dodržování vnitrostátních předpisů přijatých na základě ostatních ustanovení této směrnice, pouze pokud dotyčná třetí země zajistí

[1] The Washington Post , 31. října 2013.

odpovídající úroveň ochrany, a že účelem tohoto ustanovení je zajistit návaznost na ochranu poskytovanou právními předpisy EU o ochraně údajů v případech, kdy jsou osobní údajů předávány mimo EU;

35. připomíná, že podle směrnice 95/46/ES má být odpovídající úroveň ochrany zajišťovaná třetí zemí posuzována s ohledem na všechny okolnosti související s předáním nebo předáváním údajů; stejně tak připomíná, že uvedená směrnice uděluje rovněž Komisi prováděcí pravomoci, na jejichž základě může prohlásit, že určitá třetí země zajišťuje odpovídající úroveň ochrany podle kritérií stanovených směrnicí 95/46/ES; směrnice 95/46/ES nicméně také Komisi umožňuje prohlásit, že určitá třetí země odpovídající úroveň ochrany nezajišťuje;

36. připomíná, že ve druhém uvedeném případě musí členské státy přijmout nezbytná opatření, kterými zabrání jakémukoli předávání údajů téhož druhu do dotčené třetí země, a že Komise by měla zahájit jednání za účelem nápravy této situace;

37. vyzývá Komisi a členské státy, aby bezodkladně posoudily, zda odpovídající úroveň ochrany zajišťovaná novozélandským a kanadským zákonem o ochraně osobních informací a elektronických dokumentech a potvrzená Komisí v rozhodnutí 2013/65[1] a rozhodnutí 2/2002 ze dne 20. prosince 2001 nebyla oslabena účastí národních zpravodajských agentur těchto zemí v hromadném sledování občanů EU, a dále ji vyzývá, aby případně přijala náležitá opatření k pozastavení platnosti nebo ke změně rozhodnutí o odpovídající ochraně; očekává, že Komise bude Evropský parlament nejpozději do prosince 2014 informovat o svých zjištěních ohledně výše uvedených zemí;

Předávání založené na smluvních doložkách a jiných nástrojích

38. připomíná, že vnitrostátní orgány pro ochranu údajů uvedly, že standardní smluvní doložky ani závazná podniková pravidla se nezaměřují na situace, kdy je požadován přístup k osobním údajům pro účely hromadného sledování, a že zajištění tohoto přístupu by nebylo v souladu s ustanoveními smluvních doložek nebo závazných podnikových pravidel o výjimkách, která hovoří o mimořádných výjimkách za účelem legitimních zájmů v demokratické společnosti, a to pouze v nezbytných a přiměřených situacích;

39. vyzývá členské státy, aby zakázaly nebo pozastavily předávání údajů do třetích zemí na základě standardních smluvních doložek, smluvních doložek nebo závazných podnikových pravidel, jež byly schváleny příslušnými vnitrostátními orgány a v nichž se uvádí, že právní předpisy platné pro dovozce údajů stanoví požadavky, které přesahují omezení nezbytná v demokratické společnosti a mohou mít značný nepříznivý dopad na záruky poskytované platnými právními předpisy o ochraně údajů a standardními smluvními doložkami, případně aby taková předávání zakázaly nebo pozastavily, neboť jejich pokračování by pro subjekty, jichž se údaje týkají, znamenalo bezprostřední nebezpečí značného poškození;

40. vyzývá pracovní skupinu zřízenou podle článku 29, aby vydala pokyny a doporučení

[1] Úř. věst. L 28, 30.1.2013, s. 12.

ohledně záruk a mechanismů ochrany, které by měly být v zájmu zajištění ochrany soukromí, základních práv a svobod jednotlivců součástí smluvních nástrojů pro mezinárodní předávání osobních údajů z EU obzvláště s ohledem na zákony třetích zemí o zpravodajských službách a národní bezpečnosti a zapojení společností přijímajících údaje v třetí zemi do hromadného sledování prováděného zpravodajskými agenturami třetí země;

41. vyzývá Komisi, aby přezkoumala standardní smluvní doložky, které zavedla, a ověřila tak, zda zajišťují nezbytnou ochranu, pokud jde o přístup k osobním údajům předávaným na základě těchto doložek pro zpravodajské účely, a aby je případně přepracovala;

Předávání založené na dohodě o vzájemné právní pomoci

42. vyzývá Komisi, aby do konce roku 2014 důkladně posoudila platnou dohodu o vzájemné právní pomoci na základě článku 17 této dohody s cílem prověřit její uplatňování v praxi, obzvláště prověřit, zda ji Spojené státy skutečně používají k získávání informací či důkazů v EU a zda tuto dohodu neobešly, aby tak získaly informace v EU přímo, a rovněž Komisi vyzývá, aby posoudila dopad na základní práva jednotlivců; toto posouzení by se nemělo opírat pouze o oficiální prohlášení USA jako o dostatečný základ pro provedení analýzy, ale mělo by vycházet z konkrétních hodnocení EU; s cílem sladit tento nástroj s právem Unie by měl tento důkladný přezkum řešit i dopady, jaké na něj má uplatňování ústavní struktury Unie, a to obzvláště se zřetelem k protokolu 36 a článku 10 tohoto protokolu a prohlášení č. 50 k tomuto protokolu;

Vzájemná pomoc EU v trestních věcech

43. žádá Radu a Komisi, aby Parlament informovaly o tom, jak členské státy ve skutečnosti využívají Úmluvu o vzájemné pomoci v trestních věcech mezi členskými státy, zejména hlavu III této úmluvy o odposlechu telekomunikačního provozu; vyzývá Komisi, aby v souladu s prohlášením č. 50 ohledně protokolu 36 předložila do konce roku 2014 již požadovaný návrh s cílem přizpůsobit jej rámci danému Lisabonskou smlouvou;

Předávání založená na dohodě o programu pro sledování financování terorismu (TFTP) a dohodě o jmenné evidenci cestujících (PNR)

44. je toho názoru, že z informací poskytnutých Evropskou komisí a ministerstvem financí USA není jasné, zda zpravodajské služby USA získaly přístup k údajům o finančních transakcích SWIFT prováděných v EU proniknutím do sítí SWIFT nebo do operačních systémů či komunikačních sítí bank samy nebo ve spolupráci s národními zpravodajskými službami EU a bez použití stávajících dvoustranných nástrojů pro vzájemnou právní pomoc a soudní spolupráci;

45. připomíná své usnesení ze dne 23. října 2013 a žádá Komisi o pozastavení platnosti dohody o programu TFTP;

46. vyzývá Evropskou komisi, aby reagovala na obavy z toho, že tři hlavní počítačové

rezervační systémy používané leteckými společnostmi na celém světě jsou umístěny v USA a že údaje ze jmenné evidence cestujících se ukládají pomocí systémů „cloud computing“ provozovaných na území USA podle práva USA, které neposkytuje přiměřenou ochranu údajů;

Rámcová dohoda o ochraně údajů v oblasti policejní a justiční spolupráce („zastřešující dohoda“)

47. domnívá se, že nezbytnou podmínkou pro úplné obnovení vzájemné důvěry mezi transatlantickými partnery je nalezení uspokojivého řešení na základě „zastřešující dohody“;

48. žádá okamžité obnovení projednávání „zastřešující dohody“ s USA, neboť tato dohoda by měla zaručit jasně definovaná práva občanů EU a účinnou a vymahatelnou správní a soudní nápravu v USA bez jakékoli diskriminace;

49. žádá Komisi a Radu, aby neiniciovaly uzavírání žádných nových odvětvových dohod či ujednání o předávání osobních údajů pro účely vymáhání práva, dokud nevstoupí „zastřešující dohoda“ v platnost;

50. naléhavě žádá Komisi, aby do dubna 2014 podrobně informovala o jednotlivých bodech mandátu k jednání a o aktuální situaci;

Reforma ochrany údajů

51. vyzývá předsednictví Rady a většinu členských států, které podporují vysokou úroveň ochrany údajů, aby prokázaly smysl pro vedení a odpovědnost a urychlily práci na celém souboru opatření o ochraně údajů s cílem přijmout tato opatření v roce 2014 tak, aby občanům EU mohla být zajištěna lepší ochrana v nejbližší budoucnosti;

52. zdůrazňuje, že jak nařízení o ochraně údajů, tak směrnice o ochraně údajů jsou nezbytné k ochraně základních práv jednotlivců a musí se k nim tedy přistupovat jako k souboru předpisů, které mají být přijaty současně, má-li být u všech činností souvisejících se zpracováním údajů v EU zajištěna za všech okolností vysoká úroveň ochrany;

„Cloud computing“

53. konstatuje, že v důsledku výše popsaných praktik byla oslabena důvěra v „cloud computing“ v USA a v poskytovatele služeb založených na tomto systému; zdůrazňuje proto, že rozvoj evropských služeb využívajících „cloud computing“ je zásadní pro růst, zaměstnanost, důvěru v tento druh služeb a jejich poskytovatele a pro zaručení vysoké úrovně ochrany osobních údajů;

54. opakuje své vážné znepokojení nad povinným přímým poskytováním osobních údajů a informací z EU, které jsou zpracovávány podle dohod o službách využívajících „cloud computing“, orgánům třetích zemí ze strany poskytovatelů těchto služeb, kteří podléhají právním předpisům třetí země nebo využívají datové servery nacházející se ve třetích zemích, a nad přímým dálkovým přístupem k osobním údajům a informacím

zpracovávaným orgány pro vymáhání práva a zpravodajskými službami třetích zemí;

55. vyjadřuje politování nad skutečností, že tento přístup je obvykle získán tak, že orgány třetích zemí přímo prosadí uplatňování vlastních právních předpisů, aniž by byly použity mezinárodní nástroje vytvořené za účelem právní spolupráce, jako jsou dohody o vzájemné právní pomoci nebo jiné formy soudní spolupráce;

56. vyzývá Komisi a členské státy, aby urychlily úsilí o vytvoření evropského partnerství pro cloud computing;

57. připomíná, že všechny společnosti poskytující služby v EU musí bez výjimky dodržovat právní předpisy EU a nesou odpovědnost za jakékoli jejich porušení;

Transatlantické partnerství v oblasti obchodu a investic (TTIP)

58. bere na vědomí, že mezi EU a USA probíhají jednání o transatlantickém partnerství v oblasti obchodu a investic, které je mimořádně strategicky důležité pro další hospodářský růst a schopnost EU i USA určovat příští celosvětově platné regulační normy;

59. obzvláště zdůrazňuje, že s ohledem na význam digitální ekonomiky v tomto partnerství a v otázce obnovení důvěry mezi EU a USA schválí Evropský parlament konečné znění dohody o TTIP pouze tehdy, pokud bude dohoda uznávat všechna základní práva uvedená v Listině EU a pokud se bude ochrana soukromí jednotlivců v souvislosti se zpracováním a šířením osobních údajů i nadále řídit článkem XIV Všeobecné dohody o obchodu službami (GATS);

Demokratický dohled nad zpravodajskými službami

60. zdůrazňuje, že ačkoliv by se dohled nad činností zpravodajských služeb měl opírat jak o demokratickou legitimitu (silný právní rámec, povolení vydávaná ex ante a hodnocení ex post), tak i o náležité technické možnosti a náležitou odbornost, většině stávajících dohledových orgánů EU a USA oba tyto prvky rozhodně chybí, zejména jim schází technické možnosti;

61. vyzývá – podobně jako u programu Echelon – všechny národní parlamenty, které tak dosud neučinily, aby zavedly smysluplný dohled nad činností zpravodajských služeb, jejž budou vykonávat parlamentní orgány nebo odborné subjekty požívající zákonných vyšetřovacích pravomocí; vyzývá národní parlamenty, aby těmto výborům či orgánům pro dohled zajistily dostatečné zdroje, technickou odbornost a právní prostředky potřebné k účinné kontrole zpravodajských služeb;

62. vyzývá k tomu, aby v kombinaci s řádným mechanismem dohledu zajišťujícím demokratickou legitimitu a patřičné technické možnosti byla vytvořena i skupina na vysoké úrovni, jejímž účelem bude posílit spolupráci na úrovni EU v oblasti zpravodajské činnosti; zdůrazňuje, že tato skupina na vysoké úrovni by měla úzce spolupracovat s národními parlamenty v zájmu navržení dalších kroků, které je třeba přijmout pro posílení spolupráce v oblasti dohledu v EU;

63. vyzývá tuto skupinu na vysoké úrovni, aby stanovila minimální evropské normy či pokyny v oblasti dohledu nad vnitrostátními zpravodajskými službami (vykonávaného ex ante i ex post), které by vycházely ze stávajících osvědčených postupů a doporučení mezinárodních organizací (OSN, Rada Evropy);

64. vyzývá skupinu na vysoké úrovni, aby vymezila přísné limity, pokud jde o délku každého nařízeného sledování, pokud jeho pokračování řádně nezdůvodnil schvalovací či dohledový orgán;

65. vyzývá skupinu na vysoké úrovni, aby stanovila kritéria pro větší transparentnost, která by vycházela z obecné zásady přístupu k informacím a tzv. zásad z Tshwane[1];

66. má v úmyslu uspořádat do konce roku 2014 konferenci, které by se zúčastnily vnitrostátní orgány dohledu, ať už parlamentní či nezávislé;

67. vyzývá členské státy, aby se inspirovaly osvědčenými postupy za účelem zlepšení přístupu svých dohledových orgánů k informacím o zpravodajské činnosti (včetně utajovaných informací a informací pocházejících od jiných služeb) a zajištění pravomoci k provádění inspekcí na místě, rozsáhlých vyšetřovacích pravomocí, odpovídajících prostředků, dostatečných odborných znalostí, důsledné nezávislosti na vládě a povinnosti předkládat zprávy svým parlamentům;

68. vyzývá členské státy, aby rozvíjely spolupráci mezi dohledovými orgány, zejména v rámci Evropské sítě vnitrostátních kontrolorů zpravodajských služeb (ENNIR);

69. naléhavě žádá Komisi, aby do září 2014 předložila návrh právního základu pro činnost Střediska EU pro analýzu zpravodajských informací (IntCen) a vhodného mechanismu dohledu přizpůsobeného činnosti tohoto střediska, který by zahrnoval povinnost předkládat pravidelné zprávy Evropskému parlamentu;

70. vyzývá Komisi, aby do září 2014 předložila návrh na proces bezpečnostní prověrky EU pro všechny funkcionáře EU, neboť stávající systém, který vychází z bezpečnostních prověrek prováděných členským státem, jehož je daná osoba státním příslušníkem, zahrnuje rozličná kritéria a různé lhůty existující v rámci vnitrostátních systémů, takže bezpečnostní prověrky poslanců a zaměstnanců Parlamentu se provádí různými postupy v závislosti na jejich státní příslušnosti;

71. připomíná ustanovení interinstitucionální dohody mezi Evropským parlamentem a Radou o předávání utajovaných informací v držení Rady, jež se týkají záležitostí mimo oblast společné zahraniční a bezpečnostní politiky, Evropskému parlamentu a o jeho nakládání s nimi,

Agentury EU

72. vyzývá společný kontrolní orgán Europolu a vnitrostátní orgány pro ochranu údajů, aby do konce roku 2014 provedly společnou inspekci s cílem zjistit, zda informace a osobní údaje sdílené s Europolem nabyly vnitrostátní orgány zákonně, zejména zda

[1] Celosvětové zásady pro národní bezpečnost a právo na informace, červen 2013.

informace nebo údaje získaly původně zpravodajské služby v EU nebo ve třetí zemi a zda jsou zavedena příslušná opatření pro zamezení využívání a dalšího šíření takových informací a údajů;

73. vyzývá Europol, aby v souladu se svými pravomocemi vyzval příslušné orgány členských států, aby zahájily vyšetřování ve věci možné kyberkriminality a kybernetických útoků, kterých se vlády nebo soukromé subjekty dopustily při činnostech podléhajících kontrole;

Svoboda projevu

74. vyjadřuje hluboké znepokojení nad rostoucími hrozbami pro svobodu tisku a odrazujícími účinky, které má na novináře zastrašování ze strany státních orgánů, zejména pokud jde o ochranu důvěrnosti novinářských zdrojů; opakuje výzvy vyjádřené ve svém usnesení ze dne 21. května 2013 nazvaném „Listina základních práv EU: standardní podmínky svobody sdělovacích prostředků v celé EU“;

75. je toho názoru, že zatčení pana Mirandy a zabavení dokumentů v jeho vlastnictví podle dodatku 7 zákona o terorismu z roku 2000 (Terrosism Act 2000) a rovněž žádost, aby deník *The Guardian* tyto materiály zničil nebo odevzdal, představují narušení práva na svobodu projevu uznaného článkem 10 EÚLP a článkem 11 Listiny základních práv EU;

76. vyzývá Komisi, aby předložila návrh na komplexní rámec pro ochranu oznamovatelů v EU, v němž by obzvláštně zohlednila zvláštnosti oznamování v oblasti zpravodajských služeb, v jehož případě se mohou ustanovení týkající se finanční oblasti ukázat jako nedostačující, a poskytla silné záruky imunity;

Bezpečnost informačních technologií v EU

77. zdůrazňuje, že nedávné události jasně ukazují kritickou zranitelnost EU, a zejména orgánů EU, vnitrostátních vlád a parlamentů, velkých evropských společností, evropské infrastruktury a sítí IT, vůči důmyslným útokům prostřednictvím komplexního softwaru; bere na vědomí, že tyto útoky vyžadují takové finanční a lidské zdroje, že je pravděpodobné, že vycházejí ze státních subjektů jednajících v zastoupení zahraničních vlád nebo dokonce z určitých vnitrostátních vlád EU, které je podporují; v této souvislosti považuje případ proniknutí do systému a odposlechy telekomunikační společnosti Belgacom za znepokojivý příklad útoku na kapacity EU v oblasti IT;

78. zastává názor, že odhalení masového sledování, které způsobilo krizi, lze využít jako příležitost pro Evropu převzít iniciativu a vybudovat v střednědobém horizontu nezávislé klíčové zdroje kapacit v oblasti IT; vyzývá Komisi a členské státy, aby na podporu takových kapacit zdrojů v EU využívaly veřejné zakázky a jako klíčový požadavek ve veřejných zakázkách na zboží a služby v oblasti IT stanovily standardy EU v oblasti bezpečnosti a soukromí;

79. je hluboce znepokojen známkami toho, že zahraniční zpravodajské služby se snažily snížit bezpečnostní standardy IT a nainstalovat do řady systémů IT tzv. zadní vrátka;

80. vyzývá všechny členské státy, Komisi, Radu a Evropskou radu, aby řešily nebezpečný nedostatek nezávislosti, pokud jde o nástroje, společnosti a poskytovatele (hardwaru, softwaru, služeb a sítí) v oblasti IT v EU a kódovací a kryptografické kapacity;

81. vyzývá Komisi, normalizační orgány a agenturu ENISA, aby do září 2014 vyvinuly minimální normy v oblasti bezpečnosti a soukromí a směrnice pro systémy, sítě a služby IT, včetně služeb cloud computingu, s cílem lépe chránit osobní údajů občanů EU; je přesvědčen, že takové normy by měly být stanoveny otevřeným demokratickým postupem a neměla by je prosazovat pouze jedna země, subjekt nebo nadnárodní společnost; zastává názor, že ačkoli je třeba vzít v úvahu zákonné vymáhání právních předpisů a zájmy zpravodajských služeb s cílem podporovat boj proti terorismu, nemělo by to vést k všeobecnému oslabování spolehlivosti všech systémů IT;

82. zdůrazňuje, že telekomunikační společnosti, EU i vnitrostátní regulační orgány v oblasti telekomunikací bezpečnost IT svých uživatelů a zákazníků výslovně zanedbávaly; vyzývá Komisi, aby plně využila své stávající pravomoci podle směrnice o ochraně soukromí v odvětví elektronických komunikací a o předpisovém rámci pro telekomunikace s cílem posílit ochranu důvěrnosti komunikace přijetím opatření k zajištění toho, aby koncová zařízení byla slučitelná s právem uživatele kontrolovat a chránit své osobní údaje, a aby zjistila vysokou úroveň bezpečnosti telekomunikačních sítí a služeb, a to i tím, že bude vyžadovat kódování komunikace za pomoci nejmodernějších technologií;

83. podporuje tzv. kyberstrategii EU, je však toho názoru, že nepokrývá všechny možné hrozby a že by měla být rozšířena tak, aby se vztahovala i na jednání státu se zlým úmyslem;

84. vyzývá Komisi, aby nejpozději do ledna 2015 předložila akční plán, jehož cílem bude rozvoj větší nezávislosti EU v odvětví IT, a to včetně komplexnějšího přístupu ke zvyšování evropských technologických kapacit v oblasti IT (včetně systémů IT, vybavení, služeb, cloud computingu, kódování a anonymizace údajů), a ochrana klíčové infrastruktury IT (a to i pokud jde o vlastnictví a slabiny);

85. vyzývá Komisi, aby v rámci příštího pracovního programu v rámci programu Horizont 2020 posoudila, zda by mělo být přiděleno více prostředků na oživení evropského výzkumu, vývoje, inovací a vzdělávání v oblasti IT, zejména technologií a infrastruktury k zajištění většího soukromí, šifrování, bezpečného využívání počítačových systémů, bezpečnostních řešení s otevřeným zdrojovým kódem a informační společnosti;

86. vyzývá Komisi, aby podrobně rozvrhla současné povinnosti a nejpozději do června 2014 přezkoumala, zda centrum pro boj proti kyberkriminalitě v rámci Europolu, agentura ENISA, skupina CERT nebo úřad Evropského inspektora ochrany údajů nevyžadují širší mandát, lepší koordinaci nebo dodatečné prostředky a technické kapacity s cílem umožnit jim při vyšetřování závažných přestupků v oblasti IT v EU a při výkonu technických šetření na místě pracovat efektivněji;

87. považuje za nutné, aby EU mohla využívat podpory Akademie IT EU, která by spojila

nejlepší evropské odborníky ve všech souvisejících oborech a jejímž úkolem by bylo poskytovat všem příslušným institucím a orgánům EU odborné poradenství v oblasti IT, včetně strategií týkajících se bezpečnosti; v první řadě žádá Komisi, aby ustavila nezávislou skupinu vědeckých odborníků;

88. vyzývá sekretariát Evropského parlamentu, aby nejpozději do září 2014 provedl důkladnou analýzu a posouzení spolehlivosti, pokud jde o bezpečnost IT Evropského parlamentu, zaměřené na: rozpočtové prostředky, lidské zdroje, technické kapacity, vnitřní organizaci a všechny příslušné prvky s cílem dosáhnout vysoké úrovně bezpečnosti systémů IT v EP; je přesvědčen, že takové posouzení by mělo přinejmenším poskytnout analýzu informací a doporučení týkající se:

- nutnosti provádění pravidelných, důkladných, nezávislých bezpečnostních auditů a průnikových zkoušek prováděných za pomoci externích odborníků na bezpečnost, přičemž by byla zajištěna transparentnost a poskytnuty záruky, pokud jde o jejich nezávislost ve vztahu ke třetím zemím nebo o jiné typy přímých zájmů;

- začlenění specifických požadavků na bezpečnost/soukromí v oblasti IT do nabídkových řízení na nové systémy IT, včetně možnosti požadavku na software s otevřeným zdrojem, jako podmínky nákupu;

- seznamu podniků USA, které jsou ve smluvním vztahu s Evropským parlamentem v oblasti IT a telekomunikací, s ohledem na odhalení týkající se smluv vnitrostátních bezpečnostních orgánů se společnostmi jako je RSA, jejíž produkty Evropský parlament využívá údajně k ochraně v případě dálkového přístupu poslanců a zaměstnanců EP ke svým údajům;

- spolehlivosti a odolnosti komerčního softwaru třetích stran využívaného institucemi EU ve svých systémech IT vůči pronikání a narušování ze strany donucovacích orgánů a zpravodajských služeb EU nebo třetích zemí;

- využívání systémů s otevřeným zdrojem ve větší míře a omezení využívání standardně dostupných komerčních systémů;

- dopadu zvýšeného využívání mobilních přístrojů (chytrých telefonů, tabletů, ať již pracovně či soukromě) a jeho důsledků pro bezpečnost systému IT;

- bezpečnosti komunikace mezi jednotlivými pracovními místy Evropského parlamentu a systémy IT využívanými v Evropském parlamentu;

- využívání a umístění serverů a center IT pro systémy IT v EP a důsledky pro bezpečnost a integritu těchto systémů;

- zavádění stávajících pravidel pro narušení bezpečnosti a rychlého uvědomění příslušných orgánů poskytovateli veřejně dostupných telekomunikačních služeb do praxe;

- využívání ukládání dat EP pomocí služeb cloud computingu, a to včetně typu

ukládaných údajů, ochrany obsahu a přístupu k nim a jejich umístění, s vysvětlením příslušných právních režimů ochrany údajů;

- plánu umožňujícího využívání kódovacích technologií ve větší míře, zejména kódování ověřované po celou dobu využití všech služeb IT a komunikačních služeb, jakož i cloud computing, e-mail, výměnu rychlých zpráv a telefonování;

- využívání elektronického podpisu v e-mailech;

- analýzy přínosů vyplývajících z využívání GNU Privacy Guard jako pravidla automatického standardního šifrování e-mailů, které by současně umožnilo používat digitální podpis;

- možnosti zřízení bezpečných služeb výměny rychlých zpráv (instant messaging) v Evropském parlamentu, což by umožnilo bezpečnou komunikaci, za pomoci serveru zobrazujícího pouze zašifrovaný obsah;

89. vyzývá všechny instituce a agentury EU, aby nejpozději do prosince 2014 provedly obdobná opatření, zejména Evropská rada, Rada, Evropská služba pro vnější činnost (včetně delegací EU), Komise, Soudní dvůr a Evropská centrální banka; vyzývá členské státy, aby provedly obdobná hodnocení;

90. zdůrazňuje, že pokud jde o vnější činnost EU, měla by být v případě Evropské služby pro vnější činnost (ESVČ) provedena posouzení souvisejících rozpočtových potřeb a bezodkladně provedena první opatření a že je v návrhu rozpočtu 2015 nutné vyčlenit odpovídající prostředky;

91. je toho názoru, že řada systémů IT využívaných v oblasti svobody, bezpečnosti a práva, jako je Schengenský informační systém II, Vízový informační systém, Eurodac a další systémy v budoucnu by měly být vyvíjeny a provozovány tak, aby bylo zajištěno, že údaje nebudou v důsledku požadavků USA v rámci zákona o poskytování vhodných nástrojů pro stíhání a bránění terorismu ohroženy; vyzývá agenturu eu-LISA, aby do konce roku 2014 Parlament informovala o spolehlivosti zavedených systémů;

92. vyzývá Komisi a ESVČ, aby učinily kroky na mezinárodní úrovni, zejména ve spolupráci s OSN a dalšími zúčastněnými partnery (jako je Brazílie) a prováděly strategii EU pro demokratickou správu internetu s cílem předcházet nepřiměřenému vlivu jednotlivých subjektů, společností nebo zemí na činnosti sdružení ICANN a úřadu IANA tím, že zajistí vhodné zastoupení všech zainteresovaných stran v těchto institucích;

93. vyzývá k tomu, aby byla znovu zvážena celková struktura internetu, pokud jde o tok a ukládání údajů, přičemž by se mělo více usilovat o minimalizaci údajů a transparentnost a omezit centralizované hromadné ukládání nezpracovaných údajů a rovněž zamezit zbytečnému směrování komunikace přes země, které nesplňují základní normy, pokud jde o dodržování základních práv, ochrany údajů a soukromí;

94. vyzývá členské státy, aby ve spolupráci s agenturou ENISA, centrem pro boj proti kyberkriminalitě v rámci Europolu, skupinami CERT a vnitrostátními orgány pro ochranu údajů a útvary pro boj proti kyberkriminalitě zahájily informační kampaně pro zvyšování povědomí s cílem umožnit občanům činit informovanější rozhodnutí ohledně ukládání osobních údajů online a možností lepší ochrany, a to prostřednictvím „digitální hygieny“, kódování a bezpečného cloud computingu, přičemž by měli v plné míře využívat platformu pro informace veřejného zájmu, jež je stanovena směrnicí o univerzální službě;

95. vyzývá Komisi, aby do září 2014 posoudila možnosti vytvoření pobídek pro výrobce hardwaru a softwaru, aby do svých produktů předem instalovali prvky, které by zaručovaly více bezpečnosti a větší soukromí, včetně možnosti zavedení právní odpovědnosti pro část výrobců za známé neopravené nedostatky nebo vkládání tzv. tajných zadních vrátek, a dále zvážila možnost zavedení odrazujících opatření týkajících se nepřípustného a nepřiměřeného hromadného sběru osobních údajů a případně předložila legislativní návrhy;

Obnovení důvěry

96. je přesvědčen, že toto šetření ukázalo, že je nutné, aby se USA a jejich partneři snažili obnovit vzájemnou důvěru, jelikož se jedná především o činnost zpravodajských agentur USA;

97. zdůrazňuje, že krize důvěry měla vliv:

– na atmosféru spolupráce v rámci EU, jelikož některé vnitrostátní činnosti zpravodajských služeb mohou ohrozit dosažení cílů Unie;

– na občany, kteří zjistili, že je mohou sledovat nejen třetí země či nadnárodní společnosti, ale rovněž vláda jejich země;

– na dodržování zásad právního státu a důvěryhodnost demokratických záruk v digitální společnosti;

Mezi EU a USA

98. připomíná historický i strategický význam partnerství mezi členskými státy EU a USA založeného na společné víře v demokracii, právní stát a základní práva;

99. je přesvědčen že hromadné sledování občanů a špionáž politických představitelů ze strany USA závažným způsobem narušilo vztahy mezi EU a USA a mělo negativní dopad na důvěru vůči organizacím USA, které působí v Evropě; to je dále umocněno tím, že v právu USA neexistují soudní a správní prostředky k nápravě, které by občané EU mohli využít, a to zejména v případech sledování pro zpravodajské účely.

100. uznává v souvislosti s globálními výzvami, kterým EU a USA čelí, že transatlantické partnerství musí být dále posíleno a že je zásadně důležité, aby transatlantická spolupráce v boji proti terorismu pokračovala; trvá nicméně na tom, že je nutné, aby USA učinily jasná opatření k obnovení důvěry a zdůraznění společných základních

hodnot, na nichž je toto partnerství založeno;

101. je připraven aktivně se podílet na dialogu se svými partnery v USA, aby se v rámci probíhajících amerických veřejných diskusí a jednání v Kongresu o reformaci sledování a přezkoumání dohledu nad bezpečnostními službami řešila práva týkající se soukromí občanů EU, aby jim byla zaručena stejná práva na informace a ochranu soukromí soudy USA a aby se změnila současná diskriminační situace;

102. trvá na tom, že je nutné provést reformy a poskytnout Evropanům účinné záruky, aby bylo zajištěno, že využívání dohledu a zpracovávání dat pro účely zahraničních zpravodajských služeb je omezeno jasně určenými podmínkami a týká se důvodných podezření nebo pravděpodobných příčin teroristických nebo nezákonných aktivit; zdůrazňuje, že tyto záměry by měly být předmětem transparentního soudního dohledu;

103. je toho názoru, že jsou potřeba jasné politické signály od našich amerických partnerů, které by ukázaly, že USA rozlišují mezi spojenci a protivníky;

104. žádá naléhavě Komisi EU a vládu USA, aby se v souvislosti s probíhajícími jednáními o zastřešující dohodě mezi EU a USA o převodu údajů pro účely vymáhání práva zabývaly právy na informace a na soudní nápravu občanů EU a uzavřely tato jednání v souladu se závazkem, který přijali ministři spravedlnosti a vnitřních věci EU a USA na svém setkání dne 18. listopadu 2013, do léta 2014;

105. vyzývá USA, aby přistoupily k Úmluvě Rady Evropy o ochraně osob s ohledem na automatizované zpracování osobních dat (Úmluva č. 108), stejně jako přistoupily k Úmluvě o kyberkriminalitě z roku 2001, a posílily tak společný právní základ transatlantických spojenců;

106. vyzývá instituce EU, aby prozkoumaly možnosti zavedení kodexu chování společně s USA, který by zaručil, že žádná špionáž ze strany USA není zaměřena na instituce a zařízení EU;

V rámci Evropské unie

107. je rovněž přesvědčen, že účast a činnost členských států EU vedly ke ztrátě důvěry; je toho názoru, že pouze plná transparentnost, pokud jde o účely a prostředky dohledu, veřejná diskuse a konečně přezkum právních předpisů, včetně posílení systému soudního a parlamentního dohledu, napomohou ztracenou důvěru obnovit;

108. je si vědom toho, že některé členské státy EU zahájily komunikaci s USA o nepodložených obviněních ze špionáže na bilaterální úrovni a že některé z nich uzavřely (Spojené království) nebo hodlají uzavřít (Německo, Francie) tzv. „ujednání o neprovádění špionáže“; zdůrazňuje, že tyto členské státy musí v plné míře sledovat zájmy EU jako celku;

109. zastává názor, že taková ujednání by neměla porušovat evropské Smlouvy, zejména zásadu upřímné spolupráce (podle čl. 4 odst. 3 SFEU), nebo celkově oslabovat politiky EU a konkrétně vnitřní trh, spravedlivou soutěž a hospodářský, průmyslový a sociální rozvoj; vyhrazuje si své právo v případě ujednání, u nichž se zjistilo, že

odporují soudržnosti Unie nebo jejími základním zásadám, o něž se opírá, zahájit postupy stanovené Smlouvami;

V mezinárodním kontextu

110. vyzývá Komisi, aby nejpozději v lednu 2015 představila strategii EU pro demokratickou správu internetu;

111. vyzývá členské státy, aby se řídily výzvou 35. mezinárodní konference komisařů pro ochranu údajů a soukromí, aby podporovali přijetí dodatečného protokolu k článku 7 Mezinárodního paktu o občanských a politických právech (ICCPR) na základě standardů, které byly vyvinuty a schváleny mezinárodní konferencí, a ujednání v obecné připomínce č. 16 k mezinárodnímu paktu s cílem vytvořit globálně použitelné standardy pro ochranu údajů a soukromí v souladu se zásadami právního státu; vyzývá vysokou představitelku, místopředsedkyni Komise a Evropskou službu pro vnější činnost, aby k této záležitosti zaujaly aktivní postoj;

112. vyzývá členské státy, aby v rámci Organizace spojených národů vyvinuly ucelenou a přesvědčivou strategii, která by podpořila zejména usnesení nazvané „Právo na soukromí v digitálním věku“ iniciované Brazílií a Německem a přijaté dne 27. listopadu 2013 třetím výborem Valného shromáždění OSN (výborem pro lidská práva);

Seznam priorit: Evropský digitální habeas corpus

113. rozhodl se předložit občanům EU, institucím a členským státům výše uvedená doporučení jako seznam priorit pro následující volební období;

114. rozhodl se zahájit *Evropský digitální habeas corpus pro ochranu soukromí* vycházející z následujících 7 opatření Evropského parlamentu jako dohlížecího orgánu:

Opatření 1: přijmout v roce 2014 balíček opatření na ochranu údajů;

Opatření 2: uzavřít zastřešující dohodu mezi EU a USA zajišťující řádné mechanismy nápravy pro občany EU v případě převodu údajů z EU do USA pro účely vymáhání práva;

Opatření 3: zastavit program „bezpečný přístav“, dokud nebude proveden důkladný přezkum a současné nedostatky napraveny, a zajistit, aby převody osobních údajů z Unie do USA pro komerční účely mohly probíhat výlučně podle nejvyšších standardů EU;

Opatření 4: pozastavit platnost dohody o programu TFTP do i) ukončení jednání o zastřešující dohodě; ii) dokončení důkladného šetření na základě analýzy EU a do řádného vyřešení všech připomínek vznesených Parlamentem v usnesení ze dne 23. října;

Opatření 5: chránit zásady právního státu a základní práva občanů EU, zejména se zaměřením na ohrožení svobody tisku, služebního tajemství (včetně vztahů právní

zástupce – klient) a posílené ochrany oznamovatelů;

Opatření 6: vyvinout evropskou strategii pro nezávislost IT (na vnitrostátní úrovni a úrovni EU);

Opatření 7: vybudovat postavení EU jako garanta demokratické a neutrální správy internetu;

115. vyzývá instituce EU a členské státy, aby podporovaly a prosazovaly Evropský digitální habeas corpus pro ochranu soukromí; zavazuje se převzít úlohu dohledu nad dodržováním práv občanů EU s následujícím harmonogramem monitorování provádění:

- duben–červenec 2014: monitorovací skupina, jejímž základem je vyšetřovací výbor výboru LIBE odpovědný za monitorování všech nových odhalení ve sdělovacích prostředcích týkajících se mandátu vyšetřovacího výboru a kontroly provádění tohoto usnesení;

- od července 2014: stálý mechanismus dohledu pro převody údajů a soudní nápravu v rámci příslušného výboru;

- jaro 2014: předložení výzvy Evropské radě, aby Evropský digitální hebeas corpus zahrnoval rovněž pokyny přijaté podle článku 68 SFEU;

- podzim 2014: závazek, že Evropský digitální habeas corpus a související doporučení poskytnou klíčová kritéria pro schvalování složení následujícího výboru;

- 2014–2015: pravidelné schůze skupiny pro důvěru/údaje/občanská práva složené ze zástupců Evropského parlamentu a Kongresu USA a jiných zapojených parlamentů třetích zemí, včetně Brazílie;

- 2014–2015: konference s orgány dohledu nad bezpečnostními službami parlamentů evropských států;

- 2015: konference, která by spojila špičkové evropské odborníky z různých oblastí souvisejících s bezpečností IT (včetně matematiky, kryptografie a technologií pro posílení soukromí) s cílem přispět k posílení strategie IT EU pro následující volební období;

116. pověřuje svého předsedu, aby předal toto usnesení Evropské radě, Radě, Komisi, parlamentům a vládám členských států, vnitrostátním orgánům pro ochranu údajů, Evropskému inspektorovi ochrany údajů, agentuře eu-LISA, agentuře ENISA, Agentuře pro základní práva, pracovní skupině pro ochranu údajů zřízené podle článku 29, Radě Evropy, Kongresu Spojených států amerických, vládě USA, prezidentovi, vládě a parlamentu Brazilské federativní republiky a generálnímu tajemníkovi Organizace spojených národů.

VYSVĚTLUJÍCÍ PROHLÁŠENÍ

„Úloha vládce, ať je to panovník nebo sněm, vyplývá z účelu,
pro nějž byl pověřen svrchovanou mocí,
totiž péčí o bezpečnost lidu.“
Hobbes, Leviathan (30. kapitola)

„Nemůžeme naši společnost chválit před ostatními odchylujíce se
od základních norem, které
ji činí hodnou chvály“
Lord Bingham of Cornhill,
Bývalý nejvyšší soudce Anglie a Walesu

Metodika

Od července 2013 byl vyšetřovací výbor výboru LIBE na plenárním zasedání pověřen velmi náročným úkolem[1] – provést ve velmi krátké lhůtě (za méně než 6 měsíců) šetření ve věci elektronického hromadného sledování občanů EU.

Během tohoto období uspořádal více než 15 slyšení, která byla věnována každému ze souborů témat uvedených v usnesení přijatém dne 4. července, jež se opírala o návrhy odborníků EU i USA vycházejících ze široké škály znalostí a zkušeností: institucí EU, vnitrostátních parlamentů, Kongresu USA, akademických pracovníků, novinářů, občanské společnosti, odborníků na bezpečnost a technologie a soukromého sektoru. Dále delegace výboru LIBE navštívila ve dnech 28.–30. října 2013 Washington, aby se setkala s představiteli výkonné i zákonodárné moci (akademickými pracovníky, právníky, odborníky v oblasti bezpečnosti, zástupci soukromého sektoru)[2]. Delegace Výboru pro zahraniční věci (AFET) zde byla v těchto dnech rovněž přítomna. Konalo se několik společných schůzí.

Zpravodajové společně se stínovými zpravodaji[3] z různých politických skupin a 3 členy výboru AFET[4] vypracovali řadu pracovních dokumentů[5], což umožnilo prezentaci hlavních zjištění vyšetřování. Zpravodaj by rád poděkoval stínovým zpravodajům a členům výboru AFET za jejich úzkou spolupráci a vysoké nasazení během tohoto náročného procesu.

Rozsah problému

Větší zaměření na bezpečnost a zároveň rozvoj technologií umožnil státům dozvědět se o svých občanech více než kdy dříve. Díky schopnosti shromažďovat údaje o obsahu komunikace i metadata a díky schopnosti sledovat elektronické činnosti občanů, zejména

[1] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_en.pdf
[2] Viz zpráva z delegace do Washingtonu.
[3] Seznam stínových zpravodajů: Axel Voss (PPE), Sophia in’t Veld (ALDE), Jan Philipp Albrecht (VERTS/ALE), Timothy Kirkhope (EFD), Cornelia Ernst (GUE).
[4] Seznam členů výboru AFET: José Ignacio Salafranca Sánchez-Neyra (PPE), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).
[5] Viz příloha I.

využívání chytrých telefonů a tabletových počítačů, mohou zpravodajské služby o člověku zjistit v podstatě cokoli. To **přispělo k zásadnímu posunu v práci a postupech zpravodajských agentur od tradiční koncepce cíleného sledování jakožto nezbytného a přiměřeného opatření v boji proti terorismu k systémům hromadného sledování.**

Tento proces rostoucího hromadného sledování neprošel žádnou veřejnou rozpravou ani nebyl výsledkem demokratického rozhodování. Je nutné vést diskusi o účelu a rozsahu sledování a jeho místě v demokratické společnosti. Je situace způsobená odhaleními Edwarda Snowdena znakem všeobecného společenského obratu a skutečnosti, že společnost přistoupila na to, že soukromí přestává existovat oplátkou za bezpečnost? Čelíme do té míry porušování soukromí a důvěrnosti, že je možné, že nejen pachatelé trestných činů, ale i společnosti působící v oblasti IT a zpravodajské agentury znají každý detail ze života občanů? Je možné tuto skutečnost akceptovat bez dalších diskusí? Nebo je to odpovědnost zákonodárného orgánu přizpůsobit politické a právní nástroje, které jsou k dispozici, s cílem omezit rizika a předcházet dalším škodám pro případ, že by se moci dostaly méně demokratické síly?

Reakce na hromadné sledování a veřejná diskuse

Diskuse o hromadném sledování neprobíhají uvnitř EU stejnoměrně. V mnoha členských státech veřejná diskuse vlastně téměř neprobíhá a pozornost sdělovacích prostředků se různí. Německo je, jak se zdá, zemí, kde byly reakce na odhalení nejsilnější a kde se proběhla rozsáhlá veřejná diskuse o jeho důsledcích. Ve Spojeném království a Francii se zdály být reakce navzdory šetření deníků The Guardian a Le Monde omezené, tato skutečnost byla připisována údajnému zapojení jejich vnitrostátních zpravodajských služeb do činností s NSA. Vyšetřovací výbor LIBE měl možnost vyslechnout si hodnotné příspěvky parlamentních orgánů dohledu Belgie, Nizozemska, Dánka a dokonce i Norska; britský a francouzský parlament nicméně účast odmítly. Tyto rozdíly znovu dokládají nerovnoměrnou úroveň kontrol a vyvážených pravomocí v EU v těchto otázkách a že je třeba, aby parlamentní orgány odpovědné za dohled spolupracovaly.

V návaznosti na zveřejnění odhalení Edwarda Snowdena ve sdělovacích prostředcích se veřejná diskuse zakládala na dvou typech reakcí. Na jedné straně jsou ti, kteří popírají legitimitu zveřejněných informací na základě toho, že většina zpráv ve sdělovacích prostředcích vychází z mylného výkladu; mnozí navíc pochybují, ačkoli nevyvrátili odhalení, o oprávněnosti zveřejnění z důvodu tvrzení, že tato odhalení způsobují bezpečnostní rizika v oblasti národní bezpečnosti a boje proti terorismu.

Na druhé straně jsou ti, kteří se domnívají, že poskytnuté informace vyžadují informovanou veřejnou diskusi z důvodu rozsahu problémů, které tyto informace způsobují v klíčových oblastech demokracie, včetně právního státu, základních práv, soukromí občanů, veřejné odpovědnosti orgánů pro vymáhání práva a zpravodajských služeb atd. To je jistě případ novinářů a redaktorů největších světových periodik, kteří byli o zveřejnění informováni, včetně The Guardian, Le Monde, Der Spiegel, The Washington Post a Glenn Greenwald.

Tyto dva typy reakcí popsané výše vycházejí z řady důvodů, které pokud by se vzaly v úvahu, mohou vést k úplně opačným rozhodnutím o tom, jak by EU měla nebo neměla reagovat.

Pět důvodů nejednat

– *Argument „zpravodajských služeb/vnitřní bezpečnosti EU“: mimo pravomoc EU*

Odhalení Edwarda Snowdena se týkají činnosti zpravodajských služeb USA a některých členských států. Národní bezpečnost je však v působnosti členských států, EU nemá v těchto záležitostech žádnou pravomoc (s výjimkou vnitřní bezpečnosti EU), proto není možné jednat na úrovni EU.

– *Argument „terorismu“: nebezpečí oznamovatele*

Jakákoli návazná opatření na tato odhalení nebo jejich pouhé zohlednění dále oslabují bezpečnost USA a EU, jelikož neodsuzují zveřejnění dokumentů, jejichž obsah, ačkoli je redigovaný, jak se vyjadřují mediální subjekty, může poskytnout cenné informace teroristickým skupinám.

– *Argument „velezrady“: nelegitimnost oznamovatele*

Zahájení jakékoli diskuse nebo plánování dalších opatření v návaznosti na odhalení E. Snowdena je podle některých návrhů USA a Spojeného království v podstatě neobjektivní a bezvýznamné, jelikož by byly založeny na původní velezradě.

– *Argument „realistického pohledu“: obecné strategické zájmy*

I kdyby se potvrdili určité omyly a protiprávní činnost, měla by je vyvážit potřeba udržet zvláštní vztahy mezi USA a Evropou s cílem zachovat společné hospodářské a ekonomické zájmy a zájmy v oblasti zahraniční politiky.

– *Argument „dobré správy“: důvěřuj své vládě*

Vlády USA a EU byly zvoleny demokratickým postupem. V oblasti bezpečnosti by zpravodajské služby měly zásadně dodržovat demokratické standardy, i když je jejich cílem boj proti terorismu. Tento „předpoklad dobré a zákonné správy“ závisí nejen na dobré vůli držitelů výkonných pravomocí v těchto státech, ale rovněž na mechanismech kontroly a vyváženosti, které jsou zakotveny v jejich ústavních systémech.

Lze tedy říci, že existuje řada významných důvodů, proč nejednat. To může být vysvětlením, proč se většina vlád EU po několika počátečních silných reakcích raději rozhodla dále nereagovat. Hlavní činnost Rady ministrů spočívala ve vytvoření „transatlantické skupiny odborníků na ochranu osobních údajů“, která se třikrát setkala a vypracovala závěrečnou zprávu. V rámci druhé skupiny se údajně sešly orgány USA a členských států s cílem diskutovat o otázkách zpravodajských služeb, na toto téma však nejsou dostupné žádné informace. Evropská rada se zabývala problémem sledování pouze v rámci prohlášení hlav států nebo předsedů vlád[1]. S vyšetřováním doposud začalo pouze několik vnitrostátních

[1] Závěry zasedání Evropské rady konaného ve dnech 24.–25. října 2013, zejména: „Hlavy států a předsedové vlád vzali na vědomí záměr Francie a Německa usilovat o dvoustranná jednání se Spojenými státy americkými s cílem nalézt do konce roku dohodu o vzájemných vztazích v této oblasti Vzali též na vědomí, že se další země EU mohou k této iniciativě připojit. Rovněž připomněli již existující pracovní skupinu EU a Spojených států amerických zabývající se související otázkou ochrany údajů a vyzvali k tomu, aby bylo v tomto ohledu dosaženo rychlého a konstruktivního pokroku.“

parlamentů.

Pět důvodů k jednání

– *Argument „hromadného dohledu“ – v jaké společnosti chceme žít?*

Již od úplně prvního odhalení v červnu 2013 se pravidelně odkazuje na román George Orwella „1984“. Zaměření na bezpečnost a příklon k cílenému a specifickému sledování po útocích z 11. září vážně poškozují a oslabují koncept soukromí. Dějiny Evropy i USA dokazují nebezpečí hromadného dohledu a postupného vytvoření společnosti bez soukromí.

– *Argument „základních práv“*

Hromadné a nahodilé sledování ohrožuje základní práva občanů, včetně práva na soukromí, ochranu údajů, svobodu tisku a práva na spravedlivý proces, jež jsou všechna zakotvena ve Smlouvách EU, v Listině základních práv a Úmluvě o ochraně lidských práv a základních svobod. Tato práva nelze obejít ani směnit za nějakou předpokládanou výhodu, pokud to není řádně stanoveno v právních nástrojích a v plném souladu se smlouvami.

– *Argument „vnitřní bezpečnosti EU“*

Vnitrostátní pravomoci v oblasti zpravodajství a vnitrostátní bezpečnosti nevylučují souběžné pravomoci EU. Evropská unie své pravomoci, jež jí byly v oblasti vnitřní bezpečnosti svěřeny Smlouvami EU, vykonává tím, že rozhoduje o řadě legislativních nástrojů a mezinárodních dohod zaměřených na boj proti závažné trestné činnosti a terorismu, o zavádění strategie vnitřní bezpečnosti a zřizování agentur činných v této oblasti. Dále byly vytvořeny další služby, které reagují na potřebu posílené spolupráce na úrovni EU v oblasti zpravodajství. Jedná se o INTCEN (v rámci ESVČ) a koordinátora pro boj s terorismem (v rámci generálního sekretariátu Rady), ani jeden z těchto subjektů nemá právní základ.

– *Argument „nedostatečného dohledu“*

Přestože zpravodajské služby plní při ochraně demokratické společnosti před vnitřními a vnějšími hrozbami nezastupitelnou úlohu, je třeba, aby fungovaly v rámci právního státu, a musí proto podléhat přísnému a důkladnému mechanismu dohledu. Demokratický dohled nad zpravodajskými činnostmi probíhá na vnitrostátní úrovni, ale kvůli mezinárodní povaze bezpečnostních hrozeb dochází v současnosti k masové výměně informací mezi členskými státy navzájem i s třetími zeměmi, jako jsou USA; je třeba zlepšit mechanismy dohledu jak na vnitrostátní úrovni, tak na úrovni EU, jinak se tradiční mechanismy dohledu stanou neúčinnými a zastaralými.

– *„Odrazující účinek na sdělovací prostředky“ a ochrana oznamovatelů*

Informace, které odhalil Edward Snowden, a následné mediální zprávy zdůraznily klíčovou úlohu sdělovacích prostředků v demokratických společnostech při zajišťování odpovědnosti vlád. Pokud se mechanismům dohledu nepodaří zabránit hromadnému sledování či zajistit

nápravu, stává se úloha sdělovacích prostředků a oznamovatelů při odhalování případného nezákonného jednání či zneužití moci extrémně důležitou. Reakce orgánů USA a Velké Británie směrem ke sdělovacím prostředkům ukázaly na zranitelnost sdělovacích prostředků i oznamovatelů a na naléhavou potřebu je více chránit.

Evropská unie si teď musí vybrat mezi politikou „jako obvykle“ (dostatek důvodů k tomu, aby se nejednalo, vyčkávalo a vidělo) a politikou „kontroly skutečného stavu“ (sledování není nové, existuje však dostatek důkazů o nevídaném rozsahu působnosti a pravomocí zpravodajských agentur, jež vyžadují, aby EU začala jednat).

Zásada habeas corpus ve společnosti zaměřené na sledování

V roce 1679 přijal britský parlament zákon habeas corpus, který představoval významný krok směrem k zajištění práva na soudce v dobách soupeřících jurisdikcí a střetů právních aktů. Naše demokracie v současnosti zajišťují řádná práva odsouzeným nebo zadržovaným osobám, které se osobně fyzicky účastní trestního řízení nebo jsou předvedeny před soud. Avšak údaje uvedené, zpracovávané, uchovávané a dohledatelné na digitálních sítích představují souhrn osobních údajů, tedy jakési „digitální tělo“ specifické pro každého jednotlivce, které umožňuje zjistit mnoho údajů o jeho totožnosti, různých zvycích a preferencích.

Zákon habeas corpus je uznávaným základním právním nástrojem na ochranu osobní svobody před svévolnými zásahy státu. Dnes potřebujeme tento zákon rozšířit na digitální éru. V sázce je právo na soukromí a respektování integrity a důstojnosti jednotlivce. Hromadné shromažďování údajů, při němž nejsou dodržovány předpisy EU na ochranu údajů, a konkrétní porušování zásady proporcionality při správě údajů jsou v rozporu s ústavními tradicemi členských států a se základy evropského ústavního pořádku.

Současnou novinkou je, že tato rizika vyplývají nejen z trestné činnosti (proti níž zákonodárce EU přijal řadu nástrojů) nebo z možných kybernetickým útoků vlád méně demokratických zemí. Je totiž zřejmé, že takováto rizika mohou představovat i donucovací a zpravodajské orgány demokratických zemí, které občany nebo společnosti EU dostávají do kolize norem, což vede k nižší právní jistotě, kdy může docházet k porušování práv, aniž by existovaly řádné mechanismy nápravy.

K zajištění bezpečnosti osobních údajů je nutná správa sítí. Než se vyvinuly moderní státy, nebylo možné zajistit bezpečnost na silnicích nebo v městských ulicích a fyzická integrita byla ohrožena. V dnešní době, přes bezpečnost každodenního života, nejsou informační dálnice bezpečné. Je třeba zajistit integritu digitálních údajů, a to nejen proti zločincům, ale také proti možnému zneužívání pravomocí ze strany státních orgánů nebo smluvních stran či soukromých společností v rámci tajných soudních příkazů.

Doporučení výboru LIBE k šetření

Mnoho zde uvedených problémů se velmi podobá těm, které odhalilo vyšetřování Evropského parlamentu zaměřené na program Echelon v roce 2001. Skutečnost, že tehdejší zákonodárci neměli možnost přijmout opatření v návaznosti na zjištění a doporučení, jež vyplynula z vyšetřování programu Echelon, by měla posloužit jako zásadní ponaučení pro stávající šetření. V tomto usnesení se bere v potaz rozsah odhalení i skutečnost, že k dalším odhalením stále dochází, a zaujímá se proto prozíravý přístup s cílem zajistit, aby byly připraveny

konkrétní návrhy návazných opatření pro příští volební období Parlamentu, jež zaručí, že tato zjištění zůstanou důležitým tématem v politickém programu EU.

Na základě tohoto hodnocení by zpravodaj chtěl Parlamentu předložit k hlasování následující opatření:

Evropský digitální habeas corpus na ochranu soukromí založený na sedmi opatřeních:

Opatření 1: přijmout v roce 2014 balíček opatření na ochranu údajů;

Opatření 2: uzavřít zastřešující dohodu mezi EU a USA zajišťující řádné mechanismy nápravy pro občany EU v případě předávání údajů z EU do USA pro účely vymáhání práva;

Opatření 3: pozastavit nástroj „bezpečný přístav“ dokud nebude proveden úplný přezkum a nebudou napraveny stávající právní mezery, čímž se zajistí, že předávání osobních údajů pro komerční účely z EU do USA bude možné provádět pouze v souladu s nejvyššími standardy EU;

Opatření 4: pozastavit dohodu o programu pro sledování financování terorismu dokud i) nebudou uzavřena jednání o zastřešující dohodě; ii) nebude uzavřeno podrobné šetření založené na analýze EU a nebudou řádně vyřešeny všechny obavy, které Parlament uvedl ve svém usnesení ze dne 23. října;

Opatření 5: chránit právní stát a základní práva občanů EU se zvláštním zaměřením na hrozby pro svobodu tisku a profesní důvěrnost (včetně vztahů mezi právníkem a klientem) i na posílené postavení oznamovatelů;

Opatření 6: vytvořit evropskou strategii pro nezávislost informačních technologií (na vnitrostátní úrovni i na úrovni EU);

Opatření 7: učinit z EU referenční subjekt pro demokratickou a neutrální správu internetu;

Po uzavření šetření by měl Evropský parlament i nadále jednat jako strážce práv občanů EU, a to na základě následujícího harmonogramu umožňujícího sledovat dosažený pokrok:

- duben – červenec 2014: monitorovací skupina založená na vyšetřovacím týmu výboru LIBE, jež bude sledovat veškerá nová odhalení ve sdělovacích prostředcích týkající se působnosti vyšetřování a dohlížet na provádění tohoto usnesení;

- od července 2014: stálý mechanismus dohledu pro předávání údajů a opravné prostředky v rámci příslušného výboru;

- jaro 2014: formální výzva Evropské radě, aby začlenila evropský digitální habeas corpus do pokynů, jež mají být přijaty podle článku 68 SFEU;

- podzim 2014: závazek, že evropský digitální habeas corpus a související

doporučení budou sloužit jako klíčové kritérium pro schválení příští Komise;

- 2014–2015: skupina zaměřená na důvěru, údaje a občanská práva, jež bude pravidelně svolávána a bude do ní zapojen Evropský parlament, Kongres USA i další zúčastněné parlamenty třetích zemí včetně Brazílie;

- 2014–2015: konference s evropskými orgány dohledu nad zpravodajstvím, jež jsou součástí evropských vnitrostátních parlamentů;

- 2015: konference shromažďující uznávané evropské odborníky v různých oblastech souvisejících s bezpečností informačních technologií (včetně matematiky, kryptografie, technologií na zvyšování soukromí ...) s cílem pomoci vytvořit strategii EU v oblasti informačních technologií pro příští volební období;

PŘÍLOHA I : SEZNAM PRACOVNÍCH DOKUMENTŮ

Šetření výboru LIBE

Zpravodaj a stínoví zpravodajové jako spoluautoři	Otázky	Usnesení EP ze dne 4. července 2013 (viz odstavce 15–16)
pan Moraes (S&D)	Programy sledování vytvořené USA a členskými státy EU a jejich dopad na základní práva občanů EU	16 a) b) c) d)
pan Voss (PPE)	Sledování ze strany USA, pokud jde o údaje EU, a jeho možné právní dopady na transatlantické dohody a spolupráci	16 a) b) c)
paní In't Veld (ALDE) a paní Ernst (GUE)	Demokratický dohled nad zpravodajskými službami členských států a nad zpravodajskými orgány EU	15, 16 a) c) e)
pan Albrecht (VERTS/ALE)	Vztahy mezi postupy sledování v EU a USA a ustanoveními o ochraně údajů v EU	16 c) e) f)
pan Kirkhope (ECR)	Zaměření mezinárodní, evropské i vnitrostátní bezpečnosti z perspektivy EU	16 a) b)
členové AFET 3	Zahraničněpolitické aspekty šetření elektronického hromadného sledování občanů EU	16 a) b) f)

PŘÍLOHA II: SEZNAM SLYŠENÍ A ODBORNÍKŮ

ŠETŘENÍ VÝBORU LIBE
O PROGRAMU SLEDOVÁNÍ AGENTURY NSA SPOJENÝCH STÁTŮ AMERICKÝCH ORGÁNY PRO SLEDOVÁNÍ V RŮZNÝCH ČLENSKÝCH STÁTECH A JEJICH DOPAD NA ZÁKLADNÍ PRÁVA OBČANŮ EU A NA TRANSATLANTICKOU SPOLUPRÁCI V OBLASTI SPRAVEDLNOSTI A VNITŘNÍCH VĚCÍ

Na základě usnesení Evropského parlamentu ze dne 4. července 2013 (bod 16) uskutečnil výbor LIBE sérii slyšení s cílem shromáždit informace o souvisejících aspektech, vyhodnotit dopady sledování, a to zejména na základní práva a předpisy v oblasti ochrany údajů, zkoumat mechanismy nápravy a předložit doporučení na ochranu práv občanů EU i posílení bezpečnosti informačních technologií orgánů a institucí EU.

Datum	Předmět	Odborníci
5. září 2013 15:00 – 18:30 (BXL)	– výměna názorů s novináři, kteří případ odhalili a zveřejnili související fakta	• Jacques FOLLOROU, Le Monde • Jacob APPELBAUM, investigativní novinář, vývojář softwaru a výzkumník v oblasti počítačové bezpečnost v projektu Tor • Alan RUSBRIDGER, šéfredaktor Guardian News and Media (prostřednictvím videokonference)
	– opatření navazující na činnost dočasného výboru pro odposlouchávací systém Echelon	• Carlos COELHO (poslanec EP), bývalý předseda dočasného výboru pro odposlouchávací systém Echelon • Gerhard SCHMID (bývalý poslanec EP a zpravodaj pro zprávu o systému ECHELON z roku 2001) Duncan CAMPBELL, investigativní novinář a autor zprávy STOA „Interception Capabilities 2000“
12. září 2013 10:00 – 12:00 (STR)	– zpětná vazba ze setkání transatlantické odborné skupiny EU-USA o ochraně údajů z 19.–20.	• Darius ŽILYS, předsednictví Rady, ředitel oddělení pro mezinárodní právo, litevské

	září 2013 – pracovní metoda a spolupráce v rámci šetření výboru LIBE (neveřejné jednání) – výměna názorů s pracovní skupinou pro ochranu údajů zřízenou podle článku 29	ministerstvo spravedlnosti (spolupředseda pracovní skupiny ad hoc EU-USA o ochraně údajů) • Paul NEMITZ, ředitel GŘ JUST, Evropská komise (spolupředseda pracovní skupiny ad hoc EU-USA o ochraně údajů) • Reinhard PRIEBE, ředitel GŘ HOME, Evropská komise (spolupředseda pracovní skupiny ad hoc EU-USA o ochraně údajů) • Jacob KOHNSTAMM, předseda
24.září 2013 9:00 – 11:30 a 15:00 – 18:30 (BXL) **za účasti výboru AFET**	– údajné neoprávněné proniknutí NSA do údajů systému SWIFT používaných v programu TFTP – zpětná vazba ze setkání transatlantické odborné skupiny EU-USA o ochraně údajů z 19.–20. září 2013 – výměna názorů s občanskou společností USA (část I)	• Cecilia MALMSTRÖM, členka Evropské komise • Rob WAINWRIGHT, ředitel Europolu • Blanche PETRE, vedoucí systému SWIFT • Darius ŽILYS, předsednictví Rady, ředitel oddělení pro mezinárodní právo, litevské ministerstvo spravedlnosti (spolupředseda ad hoc pracovní skupiny EU-USA o ochraně údajů) • Paul NEMITZ, ředitel GŘ JUST, Evropská komise (spolupředseda pracovní skupiny ad hoc EU-USA o ochraně údajů) • Reinhard PRIEBE, ředitel GŘ HOME, Evropská komise (spolupředseda pracovní skupiny ad hoc EU-USA o ochraně údajů) • Jens-Henrik JEPPESEN, ředitel, evropské záležitosti, Center for Democracy & Technology (CDT) • Greg NOJEIM, vedoucí právník a ředitel projektu o svobodě,

		bezpečnosti a technologii, Center for Democracy & Technology (prostřednictvím videokonference) • Dr. Reinhard KREISSL, koordinátor projektu IRISS („Increasing Resilience in Surveillance Societies“ – zvyšování odolnosti ve společnostech zaměřených na sledování) (prostřednictvím videokonference) • Caspar BOWDEN, nezávislý výzkumník, bývalý nejvyšší poradce společnosti Microsoft v oblasti soukromí, autor sdělení tematické sekce zadaného výborem LIBE o programech USA zaměřených na sledování a jejich dopadu na soukromí občanů EU
30. září 2013 15:00 – 18:30 (Bxl) **za účasti výboru AFET**	– výměna názorů s občanskou společnosti USA (část II) – činnosti oznamovatelů v oblasti dohledu a jejich právní ochrana	• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC) • Catherine CRUMP, American Civil Liberties Union (ACLU) Prohlášení oznamovatelů: • Thomas DRAKE, bývalý vedoucí pracovník NSA • J. Kirk WIEBE, bývalý vedoucí analytik NSA • Annie MACHON, bývalá zpravodajská důstojnice MI5 Prohlášení nevládních organizací o právní ochraně oznamovatelů: • Jesselyn RADACK, právnička a zástupkyně šesti oznamovatelů, Government Accountability Project • John DEVITT, Transparency International Ireland
3. října 2013 16:00 do 18:30	– údajné nabourání (hacking) / neoprávněné proniknutí britské	• pan Geert STANDAERT, místopředseda oddělení Service

(BXL)	zpravodajské služby GCHQ do systémů společnosti Belgacom	Delivery Engine, BELGACOM S.A. • pan Dirk LYBAERT, generální tajemník, BELGACOM S.A. • pan Frank ROBBEN, Commission de la Protection de la Vie Privée Belgique, spoluzpravodaj pro „dossier Belgacom“
7. října 2013 19:00 – 21:30 (STR)	– dopad programů USA zaměřených na sledování na nástroj USA bezpečný přístav – dopad programů USA zaměřených na sledování na ostatní nástroje pro mezinárodní předávání údajů (smluvní doložky, závazné podnikové předpisy)	• Dr. Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (NĚMECKO) • Christopher CONNOLLY – Galexia • Peter HUSTINX, Evropský inspektor ochrany údajů (EIOÚ) • paní Isabelle FALQUE-PIERROTIN, předsedkyně CNIL (FRANCIE)
14. října 2013 15:00 – 18:30 (BXL)	– elektronické hromadné sledování občanů EU i dalších zemí Rada Evropy a Právo EU – soudní případy v souvislosti s programy sledování	• Martin SCHEININ, bývalý zvláštní zpravodaj OSN pro prosazování a ochranu lidských práv při boji proti terorismu, profesor Evropského univerzitního institutu (EUI) a vedoucí projektu RP7 „SURVEILLE“ • soudce Bostjan ZUPANČIČ, soudce v ESLP (prostřednictvím videokonference) • Douwe KORFF, profesor práva na London Metropolitan University • Dominique GUIBERT, místopředseda „Ligue des Droits de l’Homme“ (LDH)

		• Nick PICKLES, ředitel Big Brother Watch • Constanze KURZ, informatička, vedoucí projektu ve Forschungszentrum für Kultur und Informatik
7. listopadu 2013 9:00 – 11:30 a 15:00 – 18:30 (BXL)	– úloha střediska EU IntCen ve zpravodajské činnosti EU (neveřejné jednání) – vnitrostátní programy pro hromadné sledování osobních údajů v členských státech EU a jejich soulad s právními předpisy EU – úloha parlamentního dohledu nad zpravodajskými službami na vnitrostátní úrovni v době hromadného sledování (část I) (Benátská komise) (Velká Británie) – transatlantická odborná skupina EU-USA	• pan Ilkka SALMI, ředitel Střediska EU pro analýzu zpravodajských informací (IntCen) • Dr. Sergio CARRERA, vedoucí výzkumný pracovník a vedoucí oddělení spravedlnosti a vnitřních věcí, Centrum pro evropská politická studia (CEPS), Brusel • Dr. Francesco RAGAZZI, odborný asistent v oboru mezinárodních vztahů, Univerzita v Leidenu • pan Iain CAMERON, člen Evropské komise pro demokracii prostřednictvím práva – „Benátská komise“ • pan Ian LEIGH, profesor práva, Univerzita v Durhamu • pan David BICKFORD, bývalý právní ředitel bezpečnostních a zpravodajských agentur MI5 a MI6 • pan Gus HOSEIN, výkonný ředitel, Privacy International • pan Paul NEMITZ, ředitel – základní práva a občanství, GŘ JUST, Evropská komise • pan Reinhard PRIEBE, ředitel – krizové řízení a vnitřní bezpečnost, GŘ Home, Evropská komise
11. listopadu 2013 15:00 – 18:30 (BXL)	– programy USA zaměřené na dohled a jejich dopad na soukromí občanů EU (prohlášení člena kongresu USA Jima SENSENBRENNERA)	• pan Jim SENSENBRENNER, Sněmovna reprezentantů USA (člen Committee on the Judiciary (výbor pro právní záležitosti) a předseda Subcommittee on

	– úloha parlamentního dohledu nad zpravodajskými službami na vnitrostátní úrovni v době hromadného sledování (NL, SW) (část II) – programy americké agentury NSA pro elektronické masové sledování a úloha společností v oboru informačních technologií (Microsoft, Google, Facebook)	Crime, Terrorism, Homeland Security, and Investigations (podvýbor pro trestnou činnost, terorismus, vnitřní bezpečnost a vyšetřování)) • pan Peter ERIKSSON, předseda ústavního výboru, švédský parlament (Riksdag) • pan A.H. VAN DELDEN, předseda nizozemského nezávislého přezkumného výboru pro zpravodajské a bezpečnostní služby (CTIVD) • paní Dorothee BELZ, místopředsedkyně, právní a podnikové záležitosti Microsoft EMEA (Evropa, Blízký východ a Afrika) • pan Nicklas LUNDBLAD, ředitel, styk s veřejností a vztahy s vládami, Google • pan Richard ALLAN, ředitel, styk s veřejností EMEA (Evropa, Blízký východ a Afrika), Facebook
14. listopadu 2013 15:00 – 18:30 (BXL) **za účasti výboru AFET**	– bezpečnost informačních technologií orgánů a institucí EU (část I) (EP, COM (CERT-EU), (eu-LISA) – úloha parlamentního dohledu nad zpravodajskými službami na vnitrostátní úrovni v době hromadného sledování (část III)(BE, DA)	• pan Giancarlo VILELLA, generální ředitel, GŘ ITEC, Evropský parlament • pan Ronald PRINS, ředitel a spoluzakladatel Fox-IT • pan Freddy DEZEURE, vedoucí pracovní skupiny CERT-EU, GŘ DIGIT, Evropská komise • pan Luca ZAMPAGLIONE, bezpečnostní pracovník, eu-LISA • pan Armand DE DECKER, místopředseda belgického senátu, člen monitorovacího výboru, který je součástí výboru pro dohled nad zpravodajskými službami • pan Guy RAPAILLE, předseda

		výboru pro dohled nad zpravodajskými službami (Comité R) • pan Karsten LAURITZEN, člen výboru pro právní záležitosti – mluvčí pro právní záležitosti – dánský Folketing
18. listopadu 2013 19:00 – 21:30 (STR)	– soudní případy a další stížnosti na vnitrostátní programy sledování (část II) (polská nevládní organizace)	• Dr. Adam BODNAR, místopředseda rady, Helsinská nadace pro lidská práva (Polsko)
2. prosince 2013 15:00 – 18:30 (BXL)	– úloha parlamentního dohledu nad zpravodajskými službami na vnitrostátní úrovni v době hromadného sledování (část IV) (Norsko)	• pan Michael TETZSCHNER, člen stálého výboru pro kontrolu a ústavní záležitosti, Norsko (Stortinget)
5. prosince 2013, 15:00 – 18:30 (BXL)	– bezpečnost informačních technologií orgánů a institucí EU (část II) – dopad hromadného sledování na důvěrnost vztahů mezi právníkem a klientem	• pan Olivier BURGERSDIJK, vedoucí strategie, Evropské centrum pro boj proti kyberkriminalitě, EUROPOL • Prof. Udo HELMBRECHT, výkonný ředitel agentury ENISA • pan Florian WALTHER, nezávislý konzultant v oblasti bezpečnosti informačních technologií • pan Jonathan GOLDSMITH, generální tajemník, Evropská rada advokátních komor a právnických společností (CCBE)
9. prosince 2013 (STR)	– obnovení důvěry ohledně toku údajů mezi EU-USA – rezoluce Rady Evropy 1954 (2013) o „vnitrostátní bezpečnosti a přístupu k informacím“	• paní Viviane REDING, místopředsedkyně Evropské komise • pan Arcadio DÍAZ TEJERA, člen španělského senátu, člen parlamentního shromáždění Rady Evropy a zpravodaj pro rezoluci Rady Evropy 1954 (2013) o „vnitrostátní bezpečnosti a přístupu k informacím“
17. – 18. prosince (BXL)	parlamentní výbor pro vyšetřování špionáže v brazilském senátu (videokonference)	• paní Vanessa GRAZZIOTIN, předsedkyně parlamentního výboru pro vyšetřování špionáže • pan Ricardo DE REZENDE FERRAÇO, zpravodaj

		parlamentního výboru pro vyšetřování špionáže
	prostředky informačních technologií na ochranu soukromí	• pan Bart PRENEEL, profesor počítačové bezpečnosti a průmyslové kryptografie na Katolické univerzitě v Lovani, Belgie • pan Stephan LECHNER, ředitel, institut pro ochranu a bezpečnost občana (IPSC), společné výzkumné středisko (SVS), Evropská komise • Dr. Christopher SOGHOIAN, hlavní technolog, projekt zaměřený na projev, soukromí a technologie, American Civil Liberties Union • Christian HORCHERT, konzultant v oblasti bezpečnosti informačních technologií, Německo
	výměna názorů s novinářem, který fakta zveřejnil (část II) (videokonference)	• pan Glenn GREENWALD, autor a fejetonista se zaměřením na národní bezpečnost a občanské svobody, dříve deník Guardian

PŘÍLOHA III: SEZNAM ODBORNÍKŮ, KTEŘÍ ODMÍTLI ÚČAST NA VEŘEJNÝCH SLYŠENÍCH V SOUVISLOSTI S ŠETŘENÍM VÝBORU LIBE

1. Odborníci, kteří pozvání předsedy výboru LIBE odmítli

USA

- pan Keith Alexander, generál armády USA, ředitel agentury NSA[1]
- pan Robert S. Litt, vedoucí právník, úřad ředitele národního zpravodajství[2]
- pan Robert A. Wood, chargé d'affaires, zastoupení Spojených států při Evropské unii

Spojené království

- pan Iain Lobban, ředitel agentury Government Communications Headquarters (GCHQ) Velké Británie

Francie

- pan Bajolet, Directeur général de la Sécurité Extérieure, Francie
- pan. Calvar, Directeur Central de la Sécurité Intérieure, Francie

Nizozemsko

- pan Ronald Plasterk, ministr vnitra a pro vztahy v království, Nizozemí
- pan Ivo Opstelten, ministr pro bezpečnost a obranu, Nizozemí

Polsko

- pan Dariusz Łuczak, vedoucí polské agentury pro vnitřní bezpečnost
- pan Maciej Hunia, vedoucí polské agentury pro zahraniční zpravodajství

Soukromé společnosti v oboru informačních technologií

- Tekedra N. Mawakana, globální vedoucí pro styk s veřejností a zástupce vedoucího právníka, Yahoo
- Dr Saskia Horsch, vedoucí pro styk s veřejností, Amazon

Telekomunikační společnosti EU

[1] Zpravodaj, předseda Brok a senátor Feinstein se s panem Alexanderem setkali ve Washingtonu dne 29. října 20113.
[2] Delegace výboru LIBE se s panem Littem setkala ve Washingtonu dne 29. října 2013.

- paní Doutriaux, Orange
- pan Larry Stone, předseda odboru pro veřejné a vládní záležitosti skupiny British Telecom, Velká Británie
- Telekom, Německo
- Vodafone

2. Odborníci, kteří na pozvání předsedy výboru LIBE nereagovali

Německo

- pan Gerhard Schindler, předseda Bundesnachrichtendienst (spolková zpravodajská služba)

Nizozemsko

- paní Berndsen-Jansen, Voorzitter Vaste Kamer Commissie voor Binnenlandse Zaken Tweede Kamer der Staten-Generaal, Nizozemí
- pan Rob Bertholee, ředitel Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Švédsko

- pan Ingvar Åkesson, národní obranný institut pro rádiové zpravodajství (Försvarets radioanstalt, FRA)