PARLAMENTO EUROPEU 2009 - 2014

Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

2013/2188(INI)

8.1.2014

PROJETO DE RELATÓRIO

sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos (2013/2188(INI))

Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

Relator: Claude Moraes

PR_INI_art120

Í N D I C E

Página

PROPOSTA DE RESOLUÇÃO DO PARLAMENTO EUROPEU

sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos
(2013/2188(INI))

O Parlamento Europeu,

– Tendo em conta o Tratado da União Europeia (TUE), nomeadamente os seus artigos 2.º, 3.º, 4.º, 5.º, 6.º, 7.º, 10.º, 11.º e 21.º,

– Tendo em conta o Tratado sobre o Funcionamento da União Europeia (TFUE), nomeadamente os seus artigos 15.º, 16.º e 218.º e o Título V,

– Tendo em conta o Protocolo n.º 36 relativo às disposições transitórias e o seu artigo 10.º, assim como a Declaração n.º 50 relativa a esse protocolo,

– Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente os seus artigos 1.º, 3.º, 6.º, 7.º, 8.º, 10.º, 11.º, 20.º, 21.º, 42.º, 47.º, 48.º e 52.º,

– Tendo em conta a Convenção Europeia dos Direitos do Homem, nomeadamente os seus artigos 6.º, 8.º, 9.º, 10.º e 13.º, assim como os protocolos complementares,

– Tendo em conta a Declaração Universal dos Direitos do Homem, nomeadamente os seus artigos 7.º, 8.º, 10.º, 11.º, 12.º e 14.º[1],

– Tendo em conta o Pacto Internacional sobre Direitos Civis e Políticos, nomeadamente os seus artigos 14.º, 17.º, 18.º e 19.º,

– Tendo em conta a Convenção do Conselho da Europa para a Proteção dos Dados (ETS n.º 108) e o Protocolo Adicional, de 8 de novembro de 2001, à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal no que se refere às autoridades de supervisão e aos fluxos de dados transfronteiriços (ETS n.º 181),

– Tendo em conta a Convenção do Conselho da Europa sobre a cibercriminalidade (ETS n.º 185.º),

– Tendo em conta o relatório do Relator Especial das Nações Unidas sobre a promoção e a defesa dos direitos do Homem e das liberdades fundamentais no âmbito da luta contra o terrorismo, apresentado em 17 de maio de 2010 [2],

– Tendo em conta o relatório do Relator Especial das Nações Unidas sobre a promoção e proteção do direito à liberdade de opinião e de expressão, apresentado em 17 de abril

[1] http://www.un.org/en/documents/udhr/
[2] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

de 2013[1],

– Tendo em conta as diretrizes sobre os direitos humanos e a luta contra o terrorismo, adotadas pelo Comité de Ministros do Conselho da Europa em 11 de julho de 2002,

– Tendo em conta a Declaração de Bruxelas de 1 de outubro de 2010, aprovada na 6.ª Conferência das Comissões Parlamentares sobre a Supervisão dos Serviços de Informação e Segurança dos Estados-Membros da União Europeia,

– Tendo em conta a Resolução n.º 1954 (2013) da Assembleia Parlamentar do Conselho da Europa sobre segurança nacional e acesso à informação,

– Tendo em conta o relatório sobre o controlo democrático dos serviços de segurança, adotado pela Comissão de Veneza em 11 de junho de 2007[2], e aguardando com grande interesse a sua atualização, prevista para a primavera de 2014,

– Tendo em conta os testemunhos dos representantes dos comités de supervisão dos serviços de informação da Bélgica, dos Países Baixos, da Dinamarca e da Noruega,

– Tendo em conta os processos interpostos perante os tribunais franceses[3], polacos e britânicos[4], assim como perante o Tribunal Europeu dos Direitos do Homem[5]" relativos aos sistemas de vigilância em larga escala,

– Tendo em conta a Convenção elaborada pelo Conselho em conformidade com o artigo 34.º do Tratado da União Europeia, relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia, em particular o seu Título III[6],

– Tendo em conta a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América,

– Tendo em conta os relatórios de avaliação da Comissão sobre a aplicação dos princípios de «porto seguro», de 13 de fevereiro de 2002 (SEC(2002)196) e de 20 de outubro de 2004 (SEC(2004)1323),

– Tendo em conta a Comunicação da Comissão, de 27 de novembro de 2013 (COM(2013)847), sobre o funcionamento do Porto Seguro do ponto de vista dos cidadãos da UE e das empresas estabelecidas no seu território e a Comunicação da Comissão, de 27 de novembro de 2013, sobre o restabelecimento da confiança nos fluxos de dados UE-EUA (COM(2013)846),

---

[1] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
[2] http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
[3] La Fédération Internationale des Ligues des Droits de l'Homme e La Ligue française pour la défense des droits de l'Homme et du Citoyen contra X; Tribunal de Grande Instance de Paris.
[4] Processos interpostos pela Privacy International e Liberty perante o Investigatory Powers Tribunal.
[5] Pedido conjunto ao abrigo do artigo 34.º de Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz (Requerentes) contra o Reino Unido (Requerido).
[6] JO C 197 de 12.7.2000, p. 1.

– Tendo em conta a Resolução do Parlamento Europeu, de 5 de julho de 2000, sobre o projeto de decisão da Comissão relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidas pelo «Department of Commerce» dos EUA, que considerou não ser possível confirmar a adequação do sistema[1], assim como os pareceres do Grupo de Trabalho do artigo 29.º, em particular o Parecer 4/2000 de 16 de maio de 2000[2],

– Tendo em conta os acordos entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros (Acordo PNR) de 2004, 2007[3] e 2012[4],

– Tendo em conta a revisão conjunta da implementação do acordo entre a UE e os EUA sobre o tratamento e a transferência de registos de identificação dos passageiros para o Departamento da Segurança Interna dos EUA[5], que acompanha o relatório da Comissão ao Parlamento Europeu e ao Conselho sobre a revisão conjunta (COM(2013)844),

– Tendo em conta as conclusões do Advogado-Geral Pedro Cruz Villalón, segundo as quais a Diretiva 2006/24/CE relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações é, no seu conjunto, incompatível com o artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia e o seu artigo 6.º é incompatível com o artigo 7.º e o artigo 52.º, n.º 1, da Carta[6],

– Tendo em conta a Decisão 2010/412/UE do Conselho, de 13 de julho de 2010, relativa à celebração do Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Deteção do Financiamento do Terrorismo (TFTP)[7] e as declarações da Comissão Europeia e do Conselho que a acompanham,

– Tendo em conta o Acordo entre a União Europeia e os Estados Unidos da América sobre auxílio judiciário mútuo[8],

– Tendo em conta as negociações em curso sobre o acordo-quadro UE-EUA sobre a proteção de dados pessoais transferidos e tratados para efeitos de prevenção, investigação, deteção e repressão de crimes, incluindo o terrorismo, no contexto da cooperação policial e judiciária em matéria penal («acordo global»).

– Tendo em conta o Regulamento (CE) n.º 2271/96 do Conselho, de 22 de novembro de

[1] JO C 121 de 24.04.01, p. 152.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
[3] JO L 204 de 4.8.2007, p. 18.
[4] JO L 215 de 11.08.12, p. 5.
[5] SEC(2013) 630, 27.11.2013.
[6] Conclusões do Advogado-Geral Pedro Cruz Villalón, apresentadas em 12 de dezembro de 2013, no processo C-293/12.
[7] JO L 195 de 27.07.10, p. 3.
[8] JO L 181 de 19.7.2003, p. 34.

1996, relativo à proteção contra os efeitos da aplicação extraterritorial de legislação adotada por um país terceiro e das medidas nela baseadas ou dela resultantes[1],

– Tendo em conta a declaração da Presidente da República Federativa do Brasil por ocasião da abertura da 68.ª sessão da Assembleia Geral da ONU, em 24 de setembro de 2013, e o trabalho realizado pela Comissão Parlamentar de Inquérito sobre a espionagem, estabelecida pelo Senado Federal do Brasil,

– Tendo em conta o «PATRIOT Act» dos EUA, assinado pelo Presidente George W. Bush em 26 de outubro de 2001,

– Tendo em conta o «Foreign Intelligence Surveillance Act» (FISA) de 1978 e o «FISA Amendments Act» de 2008,

– Tendo em conta o decreto n.º 12333, emitido pelo Presidente dos EUA em 1981 e alterado em 2008,

– Tendo em conta as propostas legislativas atualmente em análise no Congresso dos EUA, em particular o projeto de «US Freedom Act»,

– Tendo em conta as revisões realizadas pela Comissão de Controlo da Privacidade e das Liberdades Cívicas (Privacy and Civil Liberties Oversight Board), pelo Conselho de Segurança Nacional (National Security Council) dos EUA e pelo Grupo Consultivo do Presidente sobre Serviços de Informação e Tecnologias da Comunicação (President's Review Group on Intelligence and Communications Technology), em particular o relatório deste último, de 12 de dezembro de 2013, intitulado «Liberty and Security in a Changing World» (Liberdade e Segurança num Mundo em Mudança),

– Tendo em conta o acórdão da United States District Court for the District of Columbia (Tribunal Distrital dos Estados Unidos para o distrito de Colúmbia), Klayman et al. contra Obama et al., Processo civil n.º 13-0851, de 16 de dezembro de 2013,

– Tendo em conta o relatório sobre as constatações dos copresidentes da UE do grupo de trabalho *ad hoc* UE-EUA sobre a proteção de dados, de 27 de novembro de 2013[2],

– Tendo em conta as suas resoluções, de 5 de setembro de 2001 e de 7 de novembro de 2002, sobre a existência de um sistema mundial para a interceção de comunicações privadas e comerciais (sistema de interceção ECHELON),

– Tendo em conta a sua Resolução, de 21 de maio de 2013, sobre a Carta da UE: enquadramento geral da liberdade nos meios de comunicação social na UE[3],

– Tendo em conta a sua Resolução, de 4 de julho de 2013, sobre o programa de vigilância da Agência Nacional de Segurança dos Estados Unidos, os órgãos de vigilância em diversos Estados-Membros e o seu impacto na privacidade dos cidadãos da UE, na qual encarregou a sua Comissão das Liberdades Cívicas, da Justiça e dos

[1] JO L 309, de 29.11.1996, p. 1.
[2] Documento 16987/13 do Conselho.
[3] Textos aprovados, P7_TA(2013)0203.

Assuntos Internos de conduzir um inquérito aprofundado sobre a questão[1],

– Tendo em conta a sua Resolução, de 23 de outubro de 2013, sobre a criminalidade organizada, a corrupção e o branqueamento de capitais: recomendações sobre medidas e iniciativas a desenvolver[2],

– Tendo em conta a sua Resolução, de 23 de outubro de 2013, sobre a suspensão do Acordo TFTP em consequência da vigilância exercida pela Agência Nacional de Segurança dos EUA[3],

– Tendo em conta a sua Resolução, de 10 de dezembro de 2013, sobre a exploração plena do potencial da computação em nuvem na Europa[4],

– Tendo em conta o Acordo Interinstitucional entre o Parlamento Europeu e o Conselho sobre o envio ao Parlamento Europeu e o tratamento por parte deste de informações classificadas na posse do Conselho relativas a matérias não abrangidas pela Política Externa e de Segurança Comum[5],

– Tendo em conta o Anexo VIII do seu Regimento,

– Tendo em conta o artigo 48.º do seu Regimento,

– Tendo em conta o relatório da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (A70000/2013),

O impacto da vigilância em larga escala

A. Considerando que os laços entre a Europa e os Estados Unidos da América se baseiam no espírito e nos princípios da democracia, da liberdade, da justiça e da solidariedade;

B. Considerando que a confiança e o entendimento mútuos são fatores fundamentais no diálogo transatlântico;

C. Considerando que, em setembro de 2001, o mundo entrou numa nova fase que resultou na colocação da luta contra o terrorismo entre as principais prioridades da maioria dos governos; considerando que as revelações baseadas nos documentos divulgados por Edward Snowden, antigo colaborador da NSA, obrigam os líderes democraticamente eleitos a abordar os desafios do aumento das capacidades das agências de informação em atividades de vigilância, assim como as suas implicações para o Estado de direito numa sociedade democrática;

D. Considerando que as revelações feitas desde junho de 2013 têm causado várias preocupações na UE no que diz respeito:

[1] Textos Aprovados, P7_TA(2013)0322.
[2] Textos aprovados, P7_TA(2013)0444.
[3] Textos aprovados, P7_TA(2013)0449.
[4] Textos aprovados, P7_TA(2013)0535.
[5] JO C 353 E de 03.12.13, p. 156-167.

- À dimensão dos sistemas de vigilância revelados nos EUA e nos Estados-Membros da UE;
- Ao elevado risco de violação das normas jurídicas da UE, dos direitos fundamentais e das normas de proteção de dados;
- Ao grau de confiança entre os parceiros transatlânticos da UE e dos EUA;
- Ao grau de cooperação e envolvimento de certos Estados-Membros da UE nos programas de vigilância dos EUA ou em programas equivalentes a nível nacional revelados pelos meios de comunicação social;
- Ao grau de controlo e supervisão eficaz exercido pelas autoridades políticas dos EUA e por certos Estados-Membros da UE sobre as suas comunidades de informação;
- À possibilidade de estas operações de vigilância em larga escala serem utilizadas por motivos não relacionados com a segurança nacional e a luta contra o terrorismo, designadamente para espionagem económica e industrial ou para definição de perfis para fins políticos;
- Aos respetivos papéis e grau de envolvimento das agências de informação e das empresas privadas de informática e telecomunicações;
- Às fronteiras cada vez menos nítidas entre as atividades de aplicação da lei e de informação, levando a que todos os cidadãos sejam tratados como suspeitos;
- Às ameaças à privacidade na era digital;

E. Considerando que a magnitude sem precedentes da espionagem revelada requer um inquérito aprofundado pelas autoridades dos EUA, pelas instituições europeias e pelos governos e parlamentos nacionais dos Estados-Membros;

F. Considerando que as autoridades dos EUA negaram algumas das informações reveladas, mas não contestaram a maior parte destas informações; considerando que se desenvolveu um debate público a larga escala nos EUA e num número limitado de Estados-Membros da UE; considerando que os governos da UE se mantêm demasiadas vezes em silêncio, abstendo-se de lançar inquéritos adequados;

G. Considerando que as Instituições Europeias têm o dever de assegurar que o direito da UE seja plenamente aplicado a favor dos cidadãos europeus e que a força jurídica dos Tratados da UE não seja comprometida por uma aceitação arrogante dos efeitos extraterritoriais das normas ou ações de países terceiros;

Desenvolvimentos nos EUA sobre a reforma dos serviços de informação

H. Considerando que a District Court for the District of Columbia, na sua decisão de 16 de dezembro de 2013, determinou que a recolha em larga escala de metadados pela NSA constitui uma violação da Quarta Emenda da Constituição dos EUA[1];

[1] Klayman et al. contra Obama et al., Processo civil n.º 13-0851, 16 de dezembro de 2013.

I. Considerando que uma decisão da District Court for the Eastern District of Michigan (Tribunal Distrital para o distrito Leste de Michigan) determinou que a Quarta Emenda requer razoabilidade em todas as buscas, mandados prévios para todas as buscas razoáveis, mandados baseados numa causa provável preexistente, assim como particularidade no que diz respeito a pessoas, locais e coisas, e a interposição de um magistrado neutro entre os agentes do ramo executivo e os cidadãos[1];

J. Considerando que, no seu relatório de 12 de dezembro de 2013, o Grupo Consultivo do Presidente sobre Serviços de Informação e Tecnologias da Comunicação propõe 45 recomendações ao Presidente dos EUA; considerando que as recomendações salientam a necessidade de proteger, simultaneamente, a segurança nacional e a privacidade pessoal e as liberdades cívicas; considerando que, neste contexto, convida o Governo dos EUA a pôr fim, logo que tal seja viável, à recolha em larga escala de registos telefónicos de cidadãos norte-americanos ao abrigo da Secção 215 do Patriot Act, a realizar uma revisão aprofundada do quadro jurídico da NSA e dos serviços de informação dos EUA para assegurar o respeito pelo direito à privacidade, a pôr termo aos esforços envidados para subverter ou tornar vulnerável *software* comercial (funções-alçapão e *malware*), a reforçar a utilização de encriptação, em particular no caso de dados em trânsito, e a não comprometer os esforços dedicados à criação de normas de encriptação, a instituir um Advogado de Interesse Público para defender a privacidade e as liberdades cívicas junto do Tribunal de Vigilância dos Serviços de Informação Externos (Foreign Intelligence Surveillance Court), a conferir à Comissão de Controlo da Privacidade e das Liberdades Cívicas o poder de supervisionar as atividades da Comunidade de Informação no que diz respeito à informação externa e não só à luta contra o terrorismo, e de receber queixas de denunciantes, e a utilizar os Tratados de Auxílio Judiciário Mútuo para obter comunicações eletrónicas e a não recorrer à vigilância para roubar segredos industriais ou comerciais;

K. Considerando que, a respeito das atividades de informação sobre cidadãos não americanos ao abrigo da Secção 702 do FISA, as Recomendações ao Presidente dos EUA reconhecem a questão fundamental do respeito pela privacidade e pela dignidade humana consagrada no artigo 12.º da Declaração Universal dos Direitos do Homem e no artigo 17.º do Pacto Internacional sobre Direitos Civil e Políticos; considerando que não recomendam a concessão, aos cidadãos não americanos, dos mesmos direitos e proteção que são concedidos aos cidadãos norte-americanos;

Quadro jurídico

Direitos fundamentais

L. Considerando que o relatório sobre as constatações dos copresidentes da UE do grupo de trabalho *ad hoc* UE-EUA sobre a proteção de dados prevê uma panorâmica da situação jurídica dos EUA, mas não contribuiu o suficiente para estabelecer os factos relativos aos programas de vigilância dos EUA; considerando que não foi disponibilizada qualquer informação sobre a chamada «segunda via» do grupo de trabalho, no âmbito da qual os Estados-Membros discutem bilateralmente com as autoridades norte-americanas questões relacionadas com a segurança nacional;

[1] ACLU contra NSA n.º 06-CV-10204, 17 de agosto de 2006.

M. Considerando que os direitos fundamentais, nomeadamente a liberdade de expressão, de imprensa, de pensamento, de consciência, de religião e de associação, o direito à vida privada, à proteção dos dados e à ação, a presunção de inocência e o direito a um tribunal imparcial e à não-discriminação, consagrados na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia dos Direitos do Homem, são as pedras angulares da democracia;

Competências da União no domínio da segurança

N. Considerando que, nos termos do artigo 67.º, n.º 3, do TFUE, a UE «envida esforços para garantir um elevado nível de segurança»; considerando que as disposições dos Tratados (em particular o artigo 4.º, n.º 2, do TUE, o artigo 72.º do TFUE e o artigo 73.º do TFUE) implicam que a UE dispõe de determinadas competências em questões relacionadas com a segurança coletiva da União; considerando que a UE tem exercido competências em matéria de segurança interna decidindo quanto a uma série de instrumentos legislativos e celebrando acordos internacionais (PNR, TFTP) destinados a combater os crimes graves e o terrorismo, bem como criando uma estratégia de segurança interna e agências que operam neste domínio;

O. Considerando que os conceitos de «segurança nacional», «segurança interna», «segurança interna da UE» e «segurança internacional» se sobrepõem; considerando que a Convenção de Viena sobre o Direito dos Tratados, o princípio da cooperação leal entre os Estados-Membros da UE e o princípio de interpretação das isenções previsto na legislação em matéria de direitos humanos apontam para uma interpretação restritiva da noção de «segurança nacional» e exigem que os Estados-Membros se abstenham de prejudicar as competências da UE;

P. Considerando que, nos termos da CEDH, as agências dos Estados-Membros e até partes privadas agindo no domínio da segurança nacional têm de respeitar os direitos nela consagrados, quer se apliquem aos seus próprios cidadãos ou aos cidadãos de outros Estados; considerando que o mesmo se aplica à cooperação com as autoridades de outros Estados no domínio da segurança nacional;

Extraterritorialidade

Q. Considerando que a aplicação extraterritorial, por um país terceiro, das suas leis, regulamentos e outros instrumentos legislativos ou executivos em situações abrangidas pela jurisdição da UE ou dos seus Estados-Membros pode influenciar o ordenamento jurídico estabelecido e o Estado de direito ou até violar o direito internacional ou da UE, incluindo os direitos das pessoas singulares e coletivas, consoante o grau e o objetivo declarado ou real de tal aplicação; considerando que, nestas circunstâncias excecionais, é necessário tomar medidas a nível da UE para garantir que o Estado de direito e os direitos das pessoas singulares e coletivas são respeitados no interior da UE, em particular eliminando, neutralizando, bloqueando ou contrariando de outra forma os efeitos da legislação estrangeira em questão;

Transferências internacionais de dados

R. Considerando que a transferência de dados pessoais pelas instituições, órgãos, serviços

ou agências da UE ou pelos Estados-Membros para os EUA para efeitos de aplicação da lei sem garantias e proteções adequadas do respeito pelos direitos fundamentais dos cidadãos da UE, em particular os direitos à privacidade e à proteção de dados pessoais, tornaria essa instituição, órgão, serviço ou agência da UE ou esse Estado-Membro responsável, nos termos do artigo 340.º do TFUE ou da jurisprudência constante do TJUE[1], por uma violação do direito da UE – que inclui qualquer violação dos direitos fundamentais consagrados na Carta da UE;

Transferências para os EUA baseadas no «porto seguro» dos EUA

S. Considerando que o quadro jurídico em matéria de proteção de dados dos EUA não garante um nível adequado de proteção dos cidadãos da UE;

T. Considerando que, a fim de permitir que os responsáveis pelo tratamento de dados da UE transfiram dados pessoais para uma entidade nos EUA, a Comissão, na sua Decisão 520/2000, declarou a adequação do nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas FAQ emitidos pelo Department of Commerce dos EUA para dados pessoais transferidos da União para organizações estabelecidas nos Estados Unidos que tenham aderido aos acordos de «porto seguro»;

U. Considerando que, na sua Resolução de 5 de julho de 2000, o Parlamento Europeu manifestou dúvidas e preocupações relativamente à adequação do «porto seguro» e convidou a Comissão a rever oportunamente a decisão à luz da experiência e da possível evolução legislativa;

V. Considerando que a Decisão 520/2000 da Comissão estipula que as autoridades competentes dos Estados-Membros podem exercer as suas competências para suspender a transferência de dados para uma organização que tenha declarado a sua adesão aos princípios de «porto seguro», a fim de proteger as pessoas no que diz respeito ao tratamento dos seus dados pessoais, no caso de existirem fortes probabilidades para supor que os princípios de «porto seguro» não estão a ser respeitados ou que a continuação da transferência dos dados pode causar graves prejuízos às pessoas em causa;

W. Considerando que a Decisão 520/2000 da Comissão também declara que, perante provas que demonstrem que os organismos responsáveis pelo cumprimento dos princípios não desempenham eficazmente as suas funções, a Comissão deve informar o Department of Commerce norte-americano e, se necessário, apresentar um projeto de medidas para revogar ou suspender a referida Decisão ou limitar o seu âmbito;

X. Considerando que, nos seus dois primeiros relatórios sobre a execução do «porto seguro», de 2002 e 2004, a Comissão identificou várias deficiências relativamente à aplicação adequada do «porto seguro» e formulou várias recomendações destinadas às autoridades dos EUA com vista à sua retificação;

Y. Considerando que, no seu terceiro relatório de execução, de 27 de novembro de 2013,

[1] Ver nomeadamente os processos apensos C-6/90 e C-9/90, Francovich e outros contra a República Italiana, acórdão de 28 de maio de 1991.

nove anos após o segundo relatório e sem que as deficiências apontadas nesse relatório tenham sido retificadas, a Comissão identificou novas fraquezas e lacunas abrangentes no «porto seguro» e concluiu que a atual execução não poderia ser mantida; considerando que a Comissão salientou que o acesso abrangente das agências de informação norte-americanas a dados transferidos para os EUA por entidades que aderiram ao «porto seguro» levanta questões graves adicionais relativas à continuidade da proteção dos dados dos titulares dos dados que são cidadãos da UE; considerando que a Comissão dirigiu 13 recomendações às autoridades norte-americanas e comprometeu-se a identificar, até ao verão de 2014, juntamente com estas autoridades, soluções a aplicar logo que possível, formando a base de uma nova revisão do funcionamento dos princípios de «porto seguro»;

Z. Considerando que, em 28-31 de outubro de 2013, a delegação da Comissão das Liberdades Civis, da Justiça e dos Assuntos Internos (Comissão LIBE) do Parlamento Europeu a Washington D.C. reuniu com o Department of Commerce e com a Comissão Federal de Comércio (Federal Trade Commission) dos EUA; considerando que o Department of Commerce reconheceu a existência de organizações que declararam ter aderido aos princípios de «porto seguro» mas que demonstram claramente um «estatuto não atual», o que significa que a empresa não cumpre os requisitos de «porto seguro», apesar de continuar a receber dados pessoais da UE; considerando que a Comissão Federal de Comércio admitiu que o «porto seguro» deveria ser revisto a fim de ser melhorado, em particular no que diz respeito aos sistemas de reclamações e resolução alternativa de litígios;

AA. Considerando que os princípios de «porto seguro» podem ser limitados à «medida necessária para observar requisitos de segurança nacional, interesse público ou execução legal»; considerando que, enquanto exceção a um direito fundamental, uma tal exceção deve ser sempre interpretada de forma restritiva e limitada ao necessário e proporcional numa sociedade democrática, devendo a lei definir claramente as condições e garantias que tornam essa limitação legítima; considerando que uma tal exceção não deve ser utilizada de forma que comprometa a proteção concedida pela legislação da UE em matéria de proteção de dados e pelo princípio de «porto seguro»;

AB. Considerando que o acesso em larga escala a informação pelas agências de informação dos EUA corroeu gravemente a confiança transatlântica e teve um impacto negativo na confiança em organizações dos EUA que atuam na UE; considerando que tal é ainda mais agravado pela falta de direitos a recurso judicial e administrativo da legislação americana para os cidadãos da UE, particularmente em casos de atividades de vigilância para efeitos de informação;

Transferências para países terceiros acompanhadas da decisão de adequação

AC. Considerando que, de acordo com as informações reveladas e com as conclusões do inquérito realizado pela Comissão LIBE, as agências de segurança nacional da Nova Zelândia e do Canadá estiveram envolvidas na vigilância em larga escala de comunicações eletrónicas e cooperaram ativamente com os EUA no chamado programa «Five Eyes», podendo ter trocado entre si dados pessoais de cidadãos da UE transferidos da UE;

AD. Considerando que as Decisões 2013/65[1] e 2/2002 da Comissão, de 20 de dezembro de 2001[2], declararam adequado o nível de proteção assegurado pela Nova Zelândia e pela lei canadiana sobre dados pessoais e documentos eletrónicos (Personal Information Protection and Electronic Documents Act); considerando que as revelações supramencionadas também afetam gravemente a confiança nos sistemas jurídicos destes países no que diz respeito à continuidade da proteção concedida aos cidadãos da UE; considerando que a Comissão não analisou este aspeto;

Transferências baseadas em cláusulas contratuais e noutros instrumentos

AE. Considerando que a Diretiva 95/46/CE prevê que as transferências internacionais para um país terceiro também podem ser realizadas através de instrumentos específicos desde que o responsável pelo tratamento estabeleça garantias adequadas para a proteção dos direitos e liberdades fundamentais e da vida privada dos indivíduos e para o exercício dos direitos correspondentes;

AF. Considerando que essas garantias podem, designadamente, resultar de cláusulas contratuais adequadas;

AG. Considerando que a Diretiva 95/46/CE confere poderes à Comissão para decidir que certas cláusulas contratuais-tipo oferecem as garantias suficientes exigidas nos termos da diretiva e considerando que, neste contexto, a Comissão adotou três modelos de cláusulas contratuais padrão para transferências para responsáveis pelo tratamento e subcontratantes (e subcontratantes ulteriores) em países terceiros;

AH. Considerando que as decisões da Comissão que estabelecem as cláusulas contratuais-tipo estipulam que as autoridades competentes dos Estados-Membros podem exercer as suas competências para suspender fluxos de dados nos casos em que esteja comprovado que a legislação a que o importador de dados ou um subcontratante ulterior está sujeito lhe impõe requisitos que lhe permitem derrogar à legislação sobre proteção de dados aplicável e que ultrapassam as restrições necessárias numa sociedade democrática, tal como previsto no artigo 13.º da Diretiva 95/46/CE, sempre que estes requisitos possam ter um efeito adverso substancial nas garantias fornecidas pela legislação sobre proteção de dados aplicável e pelas cláusulas contratuais-tipo, ou nos casos em que existam fortes probabilidades de as cláusulas contratuais-tipo constantes do anexo não estarem a ser ou não virem a ser cumpridas e de a continuação da transferência dos dados poder causar graves prejuízos aos titulares dos dados;

AI. Considerando que as autoridades nacionais de proteção de dados desenvolveram normas empresariais vinculativas destinadas a facilitar as transferências internacionais dentro de uma empresa multinacional, com garantias adequadas relativas à proteção da vida privada e dos direitos e liberdades fundamentais das pessoas relativamente ao exercício dos direitos correspondentes; considerando que, antes de serem utilizadas, as normas empresariais vinculativas têm de ser autorizadas pelas autoridades competentes dos Estados-Membros depois de estas terem avaliado a conformidade

[1] JO L 28 de 30.1.2013, p. 12.
[2] JO L 2 de 4.1.2002, p. 13.

com a legislação da União em matéria de proteção de dados;

Transferências baseadas nos acordos TFTP e PNR

AJ. Considerando que, na sua Resolução de 23 de outubro de 2013, o Parlamento Europeu manifestou sérias preocupações com os documentos revelados sobre as atividades da NSA relativas ao acesso direto a mensagens de pagamentos financeiros e dados conexos que constituiriam uma clara violação do Acordo, nomeadamente do seu artigo 1.º;

AK. Considerando que o Parlamento Europeu solicitou à Comissão que suspendesse o Acordo e solicitou que todas as informações e documentos pertinentes fossem disponibilizados de imediato para as deliberações do Parlamento;

AL. Considerando que, na sequência das alegações publicadas pelos meios de comunicação social, a Comissão decidiu abrir consultas com os EUA nos termos do artigo 19.º do Acordo TFTP; considerando que, em 27 de novembro de 2013, a Comissária Cecilia Malmström informou a Comissão LIBE de que, após ter reunido com as autoridades norte-americanas, e tendo em conta as respostas dadas por estas últimas nas suas cartas e durante as reuniões, a Comissão decidiu não prosseguir as consultas, uma vez que não existiam elementos de prova de que o Governo dos EUA tivesse agido de forma contrária ao disposto no acordo e que os EUA forneceram uma garantia por escrito em como não foi efetuada nenhuma recolha de dados direta contrária às disposições do acordo TFTP;

AM. Considerando que, durante a delegação da Comissão LIBE a Washington, em 28-31 de outubro de 2013, a delegação reuniu com o Departamento do Tesouro dos EUA; considerando que o Departamento do Tesouro dos EUA declarou que, desde a entrada em vigor do Acordo TFTP, não teve acesso a dados do SWIFT na UE, exceto no âmbito do TFTP; considerando que o Departamento do Tesouro dos EUA se recusou a comentar sobre se o acesso aos dados do SWIFT teria sido efetuado à margem do TFTP por outro órgão ou departamento governamental dos EUA ou se a administração dos EUA tinha conhecimento das atividades de vigilância em larga escala da NSA; considerando que, em 18 de dezembro de 2013, Glenn Greenwald declarou, perante o inquérito da Comissão LIBE, que a NSA e o GCHQ tinham explorado as redes da SWIFT;

AN. Considerando que as autoridades de proteção de dados belgas e neerlandesas decidiram, em 13 de novembro de 2013, realizar um inquérito conjunto à segurança das redes de pagamento da SWIFT a fim de determinar se terceiros poderiam obter acesso não autorizado ou ilegal aos dados bancários dos cidadãos europeus[1];

AO. Considerando que, de acordo com a revisão conjunta UE-EUA do Acordo PNR, o Departamento da Segurança Interna dos Estados Unidos efetuou 23 divulgações de dados PNR à NSA, numa base casuística como apoio aos casos de contra-terrorismo, consistente com os termos específicos do Acordo;

[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

AP. Considerando que a revisão conjunta não refere o facto de que, no caso do tratamento dos dados pessoais para efeitos de informação, ao abrigo da legislação americana os cidadãos não americanos não dispõem de qualquer via judicial ou administrativa para proteger os seus direitos, sendo apenas atribuídas proteções constitucionais aos cidadãos americanos; considerando que esta falta de direitos judiciais ou administrativos invalida as proteções dos cidadãos da UE previstas no Acordo PNR em vigor;

Transferências baseadas no Acordo UE-EUA sobre auxílio judiciário mútuo em matéria penal

AQ. Considerando que o Acordo UE-EUA sobre auxílio judiciário mútuo em matéria penal, de 6 de junho de 2003[1], entrou em vigor em 1 de fevereiro de 2010 e visa facilitar a cooperação entre a UE e os EUA para combater o crime de forma mais eficaz, tendo devidamente em conta os direitos individuais e o Estado de direito;

Acordo-quadro sobre proteção de dados no âmbito da cooperação policial e judicial («acordo global»)

AR. Considerando que o objetivo deste acordo global é estabelecer o quadro jurídico para todas as transferências de dados pessoais entre a UE e os EUA unicamente para efeitos de prevenção, investigação, deteção e repressão de crimes, incluindo o terrorismo, no contexto da cooperação judiciária em matéria penal; considerando que as negociações foram autorizadas pelo Conselho em 2 de dezembro de 2010;

AS. Considerando que este acordo deveria prever princípios claros e precisos, juridicamente vinculativos, em matéria de tratamento de dados, e reconhecer em particular o direito dos cidadãos da UE de aceder, retificar e eliminar os seus dados pessoais nos EUA, assim como o direito a um mecanismo eficiente de recurso administrativo e judicial para os cidadãos da UE e a uma supervisão independente das atividades de tratamento dos dados;

AT. Considerando que, na sua Comunicação de 27 de novembro de 2013, a Comissão indicou que o «acordo global» deveria resultar num elevado nível de proteção dos cidadãos de ambos os lados do Atlântico, e que deveria reforçar a confiança dos europeus nas trocas de dados UE-EUA, criando uma base sobre a qual se poderiam reforçar cooperação e a parceria UE-EUA em matéria de segurança;

AU. Considerando que as negociações sobre o acordo não progrediram devido à posição persistente do Governo dos EUA em recusar o reconhecimento de direitos eficazes de recurso administrativo e judicial para os cidadãos da UE e devido à intenção de criar amplas derrogações aos princípios de proteção de dados contidos no acordo, tais como a limitação da finalidade, a conservação de dados ou as transferências ulteriores, quer internamente quer para o estrangeiro;

Reforma de proteção de dados

AV. Considerando que o quadro jurídico da UE em matéria de proteção de dados está

[1] JO L 181 de 19.7.2003, p. 25.

atualmente a ser revisto a fim de criar um sistema abrangente, consistente, moderno e robusto para todas as atividades de tratamentos de dados na União; considerando que, em janeiro de 2012, a Comissão apresentou um pacote de propostas legislativas: um regulamento geral sobre a proteção de dados[1], que irá substituir a Diretiva 95/46/CE e estabelecer uma legislação uniforme na UE, e uma diretiva[2] que irá criar um quadro harmonizado para todas as atividades de tratamento de dados realizadas pelas autoridades de aplicação da lei para efeitos de aplicação da lei e irá reduzir a fragmentação das legislações nacionais;

AW. Considerando que, em 21 de outubro de 2013, a Comissão LIBE adotou os seus relatórios legislativos sobre as duas propostas, bem como uma decisão sobre a abertura das negociações com o Conselho com vista à adoção dos instrumentos jurídicos durante a presente legislatura;

AX. Considerando que, apesar de o Conselho Europeu de 24/25 de outubro de 2013 ter apelado à adoção atempada de um quadro geral sólido da UE para a proteção de dados, a fim de promover a confiança dos cidadãos e das empresas na economia digital, o Conselho foi incapaz de chegar a uma abordagem global sobre o regulamento geral de proteção de dados e sobre a diretiva[3];

Segurança informática e computação em nuvem

AY. Considerando que a Resolução de 10 de dezembro[4] enfatiza o potencial económico da computação em nuvem para o crescimento e o emprego;

AZ. Considerando que o nível de proteção de dados em ambiente de computação em nuvem não deve ser inferior ao exigido num outro qualquer contexto de tratamento de dados; considerando que a legislação da UE em matéria de proteção de dados, por ser tecnologicamente neutra, já é plenamente aplicável aos serviços de computação em nuvem em funcionamento na UE;

BA. Considerando que as atividades de vigilância em larga escala permitem às agências de informação aceder a dados pessoais armazenados pelos cidadãos da UE ao abrigo de acordos de serviços de computação em nuvem com importantes prestadores de serviços de computação em nuvem dos EUA; considerando que os serviços de informação norte-americanos acederam a dados pessoais armazenados em servidores localizados em solo da UE intercetando as redes internas da Yahoo e da Google[5]; considerando que estas atividades constituem uma violação das obrigações internacionais; considerando que não se exclui a possibilidade de os serviços de informação também terem tido acesso às informações armazenadas em serviços de computação em nuvem pelas autoridades públicas ou empresas e instituições dos Estados-Membros;

Controlo democrático dos serviços de informação

[1] COM(2012) 11 de 25.1.2012.
[2] COM(2012) 10 de 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf
[4] A7-0353/2013 PE506.114V2.00.
[5] The Washington Post, 31 de outubro de 2013.

BB. Considerando que os serviços de informação desempenham uma função importante na proteção da sociedade democrática contra ameaças internas e externas; considerando que os mesmos dispõem de competências e capacidades especiais para este efeito; considerando que estas competências devem ser utilizadas no respeito pelo Estado de direito, uma vez que, caso contrário, estes serviços se arriscam a perder legitimidade e a corroer a natureza democrática da sociedade;

BC. Considerando que o elevado nível de sigilo inerente aos serviços de informações, a fim de evitar que as operações em curso sejam de algum modo comprometidas, que o respetivo *modus operandi* seja revelado ou que os agentes possam correr risco de vida, impede a total transparência, o escrutínio público e a análise democrática ou o controlo jurisdicional habituais;

BD. Considerando que a evolução tecnológica levou a uma maior cooperação entre as agências de informações à escala internacional, incluindo o intercâmbio de dados pessoais, dissipando-se muitas vezes a fronteira entre as atividades de informação e de aplicação da lei;

BE. Considerando que a maioria dos mecanismos e entidades nacionais de controlo existentes foram instituídos ou reformulados na década de 1990 e não foram necessariamente adaptados à rápida evolução tecnológica da última década;

BF. Considerando que o controlo democrático das atividades de informação ainda é efetuado a nível nacional, apesar do aumento do intercâmbio de informações entre os Estados-Membros da UE e entre os Estados-Membros e países terceiros; considerando que existe um fosso cada vez maior entre o nível de cooperação internacional, por um lado, e as capacidades de controlo limitadas ao nível nacional, por outro, o que resulta num controlo democrático insuficiente e ineficaz;

Principais constatações

1. Considera que as revelações recentes na imprensa por denunciantes e jornalistas, juntamente com os dados sobre a matéria referidos por peritos durante este inquérito, resultaram em provas consistentes da existência de sistemas de longo alcance, complexos e altamente avançados em termos tecnológicos, concebidos pelos serviços de informação dos EUA e de alguns Estados-Membros, para recolher, armazenar e analisar dados e metadados de comunicação e localização de todos os cidadãos do mundo a uma escala sem precedentes e de forma indiscriminada e sem base em suspeitas;

2. Refere especificamente os programas de informação da NSA dos EUA, que permitem vigiar em larga escala os cidadãos da UE através do acesso direto aos servidores centrais das principais empresas de Internet norte-americanas (programa PRISM), analisar conteúdos e metadados (programa Xkeyscore), contornar a encriptação em linha (BULLRUN) e aceder a redes informáticas e telefónicas e a dados de localização, bem como a sistemas da agência de informação do Reino Unido GCHQ, tais como a sua atividade de vigilância a montante (programa Tempora) e o seu programa de descodificação (Edgehill); considera provável a existência de programas de natureza semelhante, mesmo a uma escala mais limitada, noutros países da UE,

como a França (DGSE), a Alemanha (BND) e a Suécia (FRA).

3. Constata as alegações de intrusão ou interceção dos sistemas Belgacom pela agência de informação do Reino Unido GCHQ; reitera a indicação da Belgacom de que não pôde confirmar se as instituições da UE foram atacadas ou afetadas, e de que o *malware* utilizado era extremamente complexo e o seu desenvolvimento e utilização exigiam a utilização de importantes recursos financeiros e humanos, o que indica que não estará disponível para entidades ou *hackers* privados;

4. Afirma que a confiança foi profundamente abalada: a confiança entre os dois parceiros transatlânticos, a confiança entre os Estados-Membros da UE, a confiança entre os cidadãos e os seus governos, a confiança no respeito pelo Estado de direito e a confiança na segurança dos serviços informáticos; acredita que, para restabelecer a confiança em todas esta dimensões, é urgentemente necessário um plano abrangente;

5. Observa que vários governos alegam que estes programas de vigilância em larga escala são necessários para combater o terrorismo; apoia incondicionalmente a luta contra o terrorismo, mas defende firmemente que esta nunca pode ser uma justificação para programas de vigilância em larga escala indiscriminados, secretos e, por vezes, até ilegais; manifesta, por conseguinte, preocupação quanto à legalidade, à necessidade e à proporcionalidade destes programas;

6. Duvida que uma recolha de dados de tal magnitude seja apenas motivada pela luta contra o terrorismo, uma vez que envolve a recolha de todos os dados possíveis de todos os cidadãos; aponta, por conseguinte, para a possível existência de outras motivações, como a espionagem política e económica;

7. Questiona a compatibilidade de certas atividades de espionagem económica em larga escala dos Estados-Membros com o mercado interno e o direito da concorrência da UE, tal como consagrado nos Títulos I e VII do Tratado sobre o Funcionamento da União Europeia; reafirma o princípio da cooperação leal consagrado no artigo 4.º, n.º 3, do Tratado da União Europeia, assim como o princípio de que os Estados-Membros se «abstêm de qualquer medida suscetível de pôr em perigo a realização dos objetivos da União»;

8. Constata que os tratados internacionais e a legislação da UE e dos EUA, assim como os mecanismos nacionais de controlo, não conseguiram garantir os controlos e equilíbrios necessários nem a responsabilização democrática;

9. Condena veementemente a recolha vasta, sistémica e generalizada de dados pessoais de cidadãos inocentes, incluindo frequentemente informações pessoais do foro íntimo; enfatiza que os sistemas de vigilância em larga escala e indiscriminada por serviços de informação interferem gravemente com os direitos fundamentais dos cidadãos; salienta que o direito à privacidade não é um luxo, mas o alicerce de uma sociedade livre e democrática; destaca ainda que a vigilância em larga escala poderá ter efeitos graves na liberdade de imprensa, de pensamento e de expressão, implicando, além disso, um potencial significativo de abuso das informações recolhidas contra adversários políticos; enfatiza que estas atividades de vigilância em larga escala parecem implicar também ações ilegais por parte dos serviços de informação e suscitar

questões relativas à extraterritorialidade das legislações nacionais;

10. Considera os programas de vigilância como mais um passo no sentido da criação de um Estado preventivo de pleno direito, mudando o paradigma estabelecido do direito penal nas sociedades democráticas, e promovendo, em vez disso, um misto de atividades de aplicação da lei e informação com garantias jurídicas pouco nítidas, muitas vezes em dissonância com os controlos e equilíbrios democráticos e com os direitos fundamentais, principalmente o da presunção da inocência; recorda, neste contexto, a decisão do Tribunal Constitucional Federal da Alemanha[1] sobre a proibição da utilização de redes de arrasto preventivas («präventive Rasterfahndung»), exceto no caso de existirem provas de perigo concreto para outros direitos importantes legalmente protegidos, e segundo a qual uma situação de ameaça global ou de tensão internacional não é suficiente para justificar este tipo de medidas;

11. Está convencido de que legislação, tratados e tribunais secretos constituem uma violação do Estado de direito; salienta que qualquer acórdão de um tribunal e qualquer decisão de uma autoridade administrativa de um Estado não pertencente à UE que autorize, direta ou indiretamente, atividades de vigilância como as analisadas por este inquérito não pode ser automaticamente reconhecido ou aplicado, devendo ser submetido, individualmente, aos procedimentos nacionais apropriados de reconhecimento mútuo e auxílio judiciário, incluindo normas impostas por acordos bilaterais;

12. Destaca que as preocupações supramencionadas são agravadas pela rápida evolução tecnológica e societal; considera que, uma vez que a Internet e os dispositivos móveis estão em todo o lado na vida quotidiana moderna («computação ubíqua») e o modelo empresarial da maioria das empresas de Internet se baseia num tratamento de dados pessoais de todo o tipo que põe em risco a integridade dos indivíduos, a dimensão deste problema não tem precedentes;

13. Considera claro, tal como enfatizado pelos peritos em tecnologia que testemunharam no inquérito, que, na fase atual de desenvolvimento tecnológico, não há qualquer garantia, quer para as instituições públicas da UE, quer para os cidadãos, de que a sua privacidade ou segurança informática possam ser protegidas contra intrusão por países terceiros bem equipados ou por agências de informação da UE («ausência de segurança informática a 100 %»); constata que esta situação alarmante apenas pode ser solucionada se os europeus estiverem dispostos a dedicar recursos suficientes, tanto humanos como financeiros, à preservação da independência e da autoconfiança da Europa;

14. Rejeita determinantemente a noção de que estas questões são puramente questões de segurança nacional e, por conseguinte, apenas da competência dos Estados-Membros; recorda um acórdão recente do Tribunal de Justiça, segundo o qual «embora seja da competência dos Estados-Membros adotarem medidas próprias para assegurar a sua segurança interna e externa, o mero facto de uma decisão dizer respeito à segurança do Estado não pode implicar a inaplicabilidade do direito da União»[2]; recorda, além

[1] 1 BvR 518/02 de 4 de abril de 2006.
[2] 1 BvR 518/02 de 4 de abril de 2006.

disso, que a proteção da privacidade de todos os cidadãos da UE está em causa, assim como a segurança e a fiabilidade de todas as redes de comunicação da UE; considera, por isso, que o debate e a ação a nível da UE não são apenas legítimos, mas também uma questão de autonomia e soberania da UE;

15. Louva os atuais debates, inquéritos e revisões relativos ao tema deste inquérito em várias partes do mundo; destaca a Global Government Surveillance Reform (Reforma Global da Vigilância do Governo), subscrita pelas principais empresas de tecnologia do mundo, que apela a alterações radicais à legislação nacional em matéria de vigilância, incluindo uma proibição à escala internacional da recolha em larga escala de dados para ajudar a preservar a confiança do público na Internet; observa com grande interesse as recomendações recentemente publicadas pelo Grupo Consultivo do Presidente dos EUA sobre Serviços de Informação e Tecnologias da Comunicação; exorta os governos a terem plenamente em conta estes apelos e recomendações e a reverem os seus quadros nacionais em matéria de serviços de informação, a fim de implementar garantias e controlos apropriados;

16. Saúda as instituições e os peritos que contribuíram para este inquérito; lamenta o facto de várias autoridades dos Estados-Membros terem declinado o convite para participar no inquérito que o Parlamento Europeu realizou em nome dos cidadãos; congratula-se com a abertura de vários membros do Congresso dos EUA e deputados dos parlamentos nacionais;

17. Está ciente de que, num período de tempo tão limitado, apenas foi possível realizar um inquérito preliminar de todas as questões em causa desde julho de 2013; reconhece a dimensão das revelações envolvidas e a sua natureza contínua; adota, por isso, uma abordagem de planeamento para o futuro, que consiste num conjunto de propostas específicas e num mecanismo de ações de acompanhamento na próxima legislatura, garantindo que as conclusões continuarão a ser prioritárias na agenda política da UE;

18. Tenciona pedir fortes compromissos políticos à Comissão Europeia, a designar após as eleições de maio de 2014, para executar as propostas e recomendações deste inquérito; espera um empenho adequado dos candidatos nas próximas audições parlamentares para os novos Comissários;

Recomendações

19. Insta as autoridades dos EUA e os Estados-Membros da UE a proibirem as atividades de vigilância em larga escala e o tratamento de grandes quantidades de dados pessoais;

20. Apela a certos Estados-Membros da UE, incluindo o Reino Unido, a Alemanha, a França, a Suécia e os Países Baixos, para que revejam, se necessário, a sua legislação nacional e as práticas que regem as atividades dos serviços de informação, a fim de garantir que estão em conformidade com as normas da Convenção Europeia dos Direitos do Homem e que cumprem as obrigações em matéria de direitos fundamentais no que diz respeito à proteção de dados, privacidade e presunção de inocência; enfatiza, em especial, dados os extensos relatórios dos meios de comunicação social relativos à vigilância em larga escala no Reino Unido, que o atual quadro jurídico, composto por uma «interação complexa» entre três atos legislativos

distintos – o Human Rights Act de 1998, o Intelligence Services Act de 1994 e o Regulation of Investigatory Powers Act de 2000 –, deve ser revisto;

21. Insta os Estados-Membros a absterem-se de aceitar dados de países terceiros que tenham sido recolhidos ilegalmente, bem como de permitir atividades de vigilância no seu território por governos ou agências de países terceiros que sejam ilegais nos termos do direito nacional ou que não cumpram as normas jurídicas consagradas nos instrumentos internacionais ou da UE, incluindo a proteção dos direitos humanos ao abrigo do TUE, da CEDH e da Carta dos Direitos Fundamentais da UE;

22. Exorta os Estados-Membros a cumprirem imediatamente a sua obrigação positiva decorrente da Convenção Europeia dos Direitos do Homem de proteger os seus cidadãos de vigilância realizada por países terceiros que seja contrária aos seus requisitos, incluindo quando o objetivo é o de salvaguardar a segurança nacional, bem como a garantirem que o Estado de direito não é enfraquecido como resultado da aplicação extraterritorial da legislação de um país terceiro;

23. Convida o Secretário-Geral do Conselho da Europa a lançar o procedimento previsto no artigo 52.º, segundo o qual «qualquer Alta Parte Contratante deverá fornecer, a requerimento do Secretário-Geral do Conselho da Europa, os esclarecimentos pertinentes sobre a forma como o seu direito interno assegura a aplicação efetiva de quaisquer disposições desta Convenção»;

24. Insta os Estados-Membros a tomarem medidas adequadas de imediato, incluindo ação judicial, contra a violação da sua soberania e, consequentemente, contra a violação do direito internacional público geral, perpetrada através dos programas de vigilância em larga escala; insta ainda os Estados-Membros da UE a utilizarem todas as medidas internacionais disponíveis para defenderem os direitos fundamentais dos cidadãos da UE, nomeadamente desencadeando o procedimento de reclamação interestatal previsto no artigo 41.º do Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP);

25. Apela aos EUA para que revejam, sem mais delongas, a sua legislação a fim de a harmonizar com o direito internacional, de reconhecer a privacidade e outros direitos dos cidadãos da UE, de prever o direito de recurso judicial para os cidadãos da UE e de assinar o Protocolo Adicional que permite a apresentação de reclamações por indivíduos ao abrigo do PIDCP;

26. Opõe-se veementemente à celebração de um protocolo ou orientações adicionais à Convenção sobre a Cibercriminalidade do Conselho da Europa (Convenção de Budapeste) sobre o acesso transfronteiras a dados armazenados em computador, que poderia prever uma legitimação do acesso dos serviços de informação a dados armazenados numa outra jurisdição sem a sua autorização e sem a utilização dos instrumentos de auxílio judiciário mútuo em vigor, uma vez que tal poderia resultar num acesso à distância ilimitado por parte das forças de segurança aos servidores e sistemas informáticos localizados noutras jurisdições, o que seria contrário à Convenção n.º 108 do Conselho da Europa;

27. Insta a Comissão a realizar, antes de julho de 2014, uma avaliação sobre a aplicabilidade do Regulamento (CE) n.º 2271/96 a casos de conflitos jurídicos em

matéria de transferências de dados pessoais;

Transferências internacionais de dados

Quadro jurídico dos EUA em matéria de proteção de dados e «porto seguro»

28. Observa que as empresas identificadas nas revelações dos meios de comunicação social como estando envolvidas na vigilância em larga escala dos titulares de dados da UE pela NSA dos EUA são empresas que declararam a sua adesão ao «porto seguro», e que o «porto seguro» é o instrumento jurídico utilizado para a transferência de dados pessoais da UE para os EUA (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); manifesta preocupação relativamente ao facto de estas organizações terem admitido que não encriptam as informações e comunicações que são transferidas entre os seus centros de dados, permitindo que estas sejam intercetadas pelos serviços de informação[1];

29. Considera que o acesso a larga escala pelas agências de informação dos EUA a dados pessoais da UE tratados pelo «porto seguro» não cumpre, por si só, os critérios de derrogação ao abrigo da «segurança nacional»;

30. Considera que, uma vez que, nas atuais circunstâncias, os princípios de «porto seguro» não asseguram a proteção adequada dos cidadãos da UE, estas transferências deveriam ser efetuadas ao abrigo de outros instrumentos, tais como cláusulas contratuais ou normas empresariais vinculativas, que prevejam garantias e proteções específicas;

31. Exorta a Comissão a apresentar medidas que prevejam a suspensão imediata da Decisão 520/2000 da Comissão, que declarou a adequação do nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas FAQ emitidos pelo Department of Commerce dos EUA;

32. Insta as autoridades competentes dos Estados-Membros, nomeadamente as autoridades de proteção de dados, a exercerem as suas competências e a suspenderem imediatamente os fluxos de dados para qualquer organização que tenha declarado a sua adesão aos princípios de «porto seguro» dos EUA, bem como a exigirem que esses fluxos de dados sejam efetuados apenas ao abrigo de outros instrumentos, desde que contenham as garantias e proteções necessárias de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas;

33. Insta a Comissão a apresentar, até junho de 2014, uma avaliação exaustiva da estrutura de privacidade dos EUA relativa a atividades comerciais, de aplicação da lei e de informação, em resposta ao facto de os sistemas jurídicos da UE e dos EUA em matéria de proteção de dados pessoais se estarem a afastar;

Transferências para outros países terceiros acompanhadas de uma decisão de adequação

34. Recorda que a Diretiva 95/46/CE estipula que a transferência para um país terceiro de dados pessoais só pode realizar-se se, sob reserva da observância das disposições

[1] *The Washington Post*, 31 de outubro de 2013.

nacionais adotadas nos termos das outras disposições da diretiva, o país terceiro em questão assegurar um nível de proteção adequado, sendo o objetivo desta disposição garantir a continuidade da proteção conferida pela legislação da UE em matéria de proteção de dados aquando da transferência de dados para fora da UE;

35. Recorda que a Diretiva 95/46/CE prevê que a adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; relembra também que a referida diretiva atribui à Comissão competências de execução para declarar que um país terceiro assegura um nível adequado de proteção à luz dos critérios previstos pela Diretiva 95/46/CE; a Diretiva 95/46/CE habilita ainda a Comissão a declarar que um país terceiro não assegura um nível adequado de proteção;

36. Recorda que, neste último caso, os Estados-Membros devem tomar as medidas necessárias para impedir qualquer transferência de dados de natureza idêntica para o país terceiro em causa, e que a Comissão deve encetar negociações com vista a obviar a situação;

37. Insta a Comissão e os Estados-Membros a avaliarem, sem mais delongas, se o nível adequado de proteção da Nova Zelândia e da lei canadiana sobre dados pessoais e documentos eletrónicos declarado pelas decisões 2013/65[1] e 2/2002 da Comissão, de 20 de dezembro de 2001, foi afetado pelo envolvimento das suas agências de informação nacionais na vigilância em larga escala dos cidadãos da UE e, se necessário, a tomarem medidas adequadas para suspender ou revogar as decisões de adequação; espera que a Comissão comunique ao Parlamento Europeu as suas conclusões relativamente aos países supramencionados o mais tardar até dezembro de 2014;

Transferências baseadas em cláusulas contratuais e noutros instrumentos

38. Recorda que as autoridades nacionais de proteção de dados indicaram que nem as cláusulas contratuais-tipo nem as normas empresariais vinculativas foram redigidas tendo em mente situações de acesso a dados pessoais para efeitos de vigilância em larga escala, e que um tal acesso não estaria em consonância com as cláusulas de derrogação das cláusulas contratuais ou das normas empresariais vinculativas que se referem a derrogações excecionais em interesse legítimo numa sociedade democrática e sempre que tal seja necessário e proporcional;

39. Solicita aos Estados-Membros que proíbam ou suspendam os fluxos de dados para países terceiros efetuados com base em cláusulas contratuais-tipo, em cláusulas contratuais ou em normas empresariais vinculativas autorizadas pelas autoridades nacionais competentes nos casos em que esteja comprovado que a legislação a que o importador de dados está sujeito lhe impõe requisitos que ultrapassam as restrições necessárias numa sociedade democrática e que possam ter um efeito adverso substancial nas garantias fornecidas pela legislação sobre proteção de dados aplicável e pelas cláusulas contratuais-tipo, ou nos casos em que a continuação da transferência dos dados cria um risco iminente de graves prejuízos aos titulares dos dados;

[1] JO L 28 de 30.1.2013, p. 12.

40. Insta o Grupo de Trabalho do Artigo 29.º a emitir orientações e recomendações sobre as garantias e proteções que os instrumentos contratuais para transferências internacionais de dados pessoais da UE devem conter a fim de assegurar a proteção da privacidade, dos direitos fundamentais e das liberdades dos indivíduos, tendo especialmente em conta a legislação de países terceiros sobre serviços de informação e segurança nacional e o envolvimento de empresas destinatárias dos dados num país terceiro em atividades de vigilância em larga escala pelas agências de informação de um país terceiro;

41. Exorta a Comissão a examinar as cláusulas contratuais-tipo que estabeleceu a fim de determinar se garantem a proteção necessária relativamente ao acesso a dados pessoais transferidos ao abrigo das cláusulas para fins de informação e, se apropriado, a revê-las;

Transferências baseadas no Acordo sobre Auxílio Judiciário Mútuo

42. Insta a Comissão a realizar, antes do final de 2014, uma avaliação aprofundada do Acordo sobre Auxílio Judiciário Mútuo em vigor, nos termos do seu artigo 17.º, a fim de verificar a sua aplicação prática e, em particular, se os EUA fizeram uso eficaz do Acordo para obter informação ou provas na UE e se o Acordo foi contornado com vista à aquisição de informação diretamente na UE, assim como a avaliar o seu impacto nos direitos fundamentais dos indivíduos; uma tal avaliação não deve apenas considerar as declarações oficiais dos EUA como uma base suficiente para análise, mas basear-se em avaliações específicas da UE; esta revisão aprofundada também deve abordar as consequências da aplicação da arquitetura constitucional da UE a este instrumento, a fim de o harmonizar com o direito da União, tendo em conta especialmente o Protocolo n.º 36 e o seu artigo 10.º, bem como a Declaração n.º 50 relativa a esse protocolo;

Auxílio mútuo na UE em matéria penal

43. Solicita ao Conselho e à Comissão que informem o Parlamento sobre a atual utilização, pelos Estados-Membros, da Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros, em particular o seu Título III relativo à interceção das telecomunicações; insta a Comissão a apresentar uma proposta, em conformidade com a Declaração n.º 50 relativa ao Protocolo n.º 36, tal como solicitado, antes do final de 2014 a fim de a adaptar ao quadro do Tratado de Lisboa;

Transferências baseadas nos acordos TFTP e PNR

44. Considera que as informações fornecidas pela Comissão Europeia e pelo Tesouro dos EUA não esclarecem se as agências de informação norte-americanas têm acesso às mensagens financeiras da SWIFT na UE intercetando as redes da SWIFT ou os sistemas operativos ou redes de comunicações dos bancos, sós ou em cooperação com as agências de informação nacionais da UE e sem recorrer aos canais bilaterais existentes de auxílio judiciário mútuo e cooperação judicial;

45. Reitera a sua Resolução de 23 de outubro de 2013 e solicita à Comissão que suspenda o Acordo TFTP;

46. Insta a Comissão Europeia a reagir às preocupações de que três dos principais sistemas informatizados de reserva utilizados pelas linhas aéreas em todo o mundo são baseados nos EUA e que os dados PNR são gravados em sistemas de computação em nuvem em funcionamento em solo americano, ao abrigo do direito dos EUA, que não é adequado em matéria de proteção de dados;

Acordo-quadro sobre proteção de dados no âmbito da cooperação policial e judicial («acordo global»)

47. Considera que uma solução satisfatória nos termos do «acordo global» é uma pré-condição para o restabelecimento total da confiança entre os parceiros transatlânticos;

48. Solicita uma retoma imediata das negociações com os EUA sobre o «acordo global», que deverá prever direitos claros para os cidadãos da UE, assim como recursos administrativos e judiciais aplicáveis nos EUA sem qualquer tipo de discriminação;

49. Solicita à Comissão e ao Conselho que não iniciem novos acordos setoriais ou mecanismos de transferência de dados pessoais para efeitos de aplicação da lei enquanto o «acordo global» não tiver entrado em vigor;

50. Exorta a Comissão a comunicar informações pormenorizadas sobre os vários pontos do mandato de negociações, assim como o último ponto da situação, até abril de 2014;

Reforma de proteção de dados

51. Insta a Presidência do Conselho e a maioria dos Estados-Membros que apoiam um elevado nível de proteção de dados a fazerem prova de um sentido de liderança e responsabilidade e acelerarem os seus trabalhos sobre o pacote relativo à proteção dos dados, a fim de permitir a sua adoção em 2014, para que os cidadãos da UE possam beneficiar de uma maior proteção num futuro muito próximo;

52. Salienta que tanto o Regulamento Proteção de Dados como a Diretiva Proteção de Dados são necessários para proteger os direitos fundamentais dos indivíduos, devendo, por isso, ser tratados como um pacote a adotar em simultâneo, a fim de assegurar que todas as atividades de tratamento de dados na UE garantem um elevado nível de proteção em quaisquer circunstâncias;

Computação em nuvem

53. Observa que a confiança na computação em nuvem e nos prestadores de serviços de computação em nuvem dos EUA foi prejudicada pelas práticas supramencionadas; enfatiza, por conseguinte, o desenvolvimento de sistemas de computação em nuvem europeus como um elemento essencial para o crescimento e o emprego e para a confiança nos serviços e nos prestadores de serviços de computação em nuvem, assim como para assegurar um elevado nível de proteção dos dados pessoais;

54. Reitera a sua séria preocupação relativamente à divulgação imediata e obrigatória de dados pessoais e de informações da UE, tratados no âmbito de acordos de computação em nuvem, a autoridades de países terceiros por prestadores de serviços de

computação em nuvem sujeitos às leis de países terceiros e relativamente ao acesso remoto direto a dados pessoais e informação tratados por autoridades policiais e serviços de informação de países terceiros;

55. Lamenta que esse acesso seja geralmente obtido através da aplicação direta por parte das autoridades de países terceiros das suas próprias normas jurídicas, sem recurso a instrumentos internacionais estabelecidos para a cooperação jurídica, tais como os acordos de auxílio judiciário mútuo (AJM) ou outras formas de cooperação judicial;

56. Insta a Comissão e os Estados-Membros a acelerarem os trabalhos com vista à criação da parceria europeia para a nuvem;

57. Salienta que todas as empresas que prestam serviços na UE devem, sem exceção, cumprir a legislação da UE e são responsáveis por quaisquer violações;

Acordo sobre a Parceria Transatlântica de Comércio e Investimento (TTIP)

58. Reconhece que a UE e os EUA estão a efetuar negociações para uma Parceria Transatlântica de Comércio e Investimento, de grande importância estratégica para um maior crescimento económico e para a capacidade da UE e dos EUA para definirem futuras normas regulamentares globais;

59. Enfatiza convictamente, dada a importância da economia digital na relação e na causa do restabelecimento da confiança UE-EUA, que o Parlamento Europeu apenas consentirá no Acordo TTIP final se este respeitar plenamente os direitos fundamentais reconhecidos pela Carta da UE, e que a proteção da privacidade dos indivíduos em relação ao tratamento e à divulgação de dados pessoais deve continuar a ser regida pelo artigo XIV do GATS;

Controlo democrático dos serviços de informação

60. Salienta que, apesar de o controlo das atividades dos serviços de informação se dever basear na legitimidade democrática (forte quadro jurídico, autorização *ex ante* e verificação *ex post*) e numa capacidade e perícia técnicas adequadas, a maioria dos atuais órgãos de controlo da UE e dos EUA demonstram uma falta dramática de ambos, em particular das capacidades técnicas;

61. Convida, tal como fez no caso do Echelon, todos os parlamentos nacionais que ainda não o fizeram a instalarem um controlo significativo das atividades de informação por entidades parlamentares ou de peritos que possuam competência jurídica para investigar; insta os parlamentos nacionais a assegurarem que essas comissões/entidades de controlo possuem recursos, perícia técnica e meios jurídicos suficientes para controlar eficazmente os serviços de informação;

62. Apela à criação de um grupo de alto nível para reforçar a cooperação no domínio da informação a nível da UE, combinado com um mecanismo adequado de controlo que assegure legitimidade democrática e uma capacidade técnica adequada; salienta que o grupo de alto nível deveria cooperar em proximidade com os parlamentos nacionais a fim de propor novas medidas com vista a um aumento da colaboração na UE em

matéria de controlo;

63. Apela a este grupo de alto nível para que defina normas ou orientações mínimas europeias sobre o controlo (*ex ante* e *ex post*) dos serviços de informação com base nas melhores práticas existentes e em recomendações de órgãos internacionais (ONU, Conselho da Europa);

64. Insta o grupo de alto nível a definir limites rigorosos para a duração de qualquer vigilância ordenada, salvo se a sua continuação for devidamente justificada pela autoridade de autorização/controlo;

65. Insta o grupo de alto nível a desenvolver critérios sobre o reforço da transparência assentes no princípio geral do acesso à informação e nos chamados «Princípios de Tshwane»[1];

66. Pretende organizar uma conferência com entidades nacionais de controlo, parlamentares ou independentes, até ao final de 2014;

67. Exorta os Estados-Membros a basearem-se nas melhores práticas para melhorarem o acesso das suas entidades de controlo às informações sobre as atividades de informação (incluindo informação classificada e informação de outros serviços) e a estabelecerem a competência para realizar visitas no local, um conjunto sólido de competências de interrogação, recursos adequados e perícia técnica, independência rigorosa perante os respetivos governos e uma obrigação de comunicação de informações aos respetivos parlamentos;

68. Insta os Estados-Membros a desenvolverem a cooperação entre as entidades de controlo, em particular no âmbito da Rede Europeia de Analistas Nacionais de Informações (ENNIR);

69. Exorta a Comissão a apresentar, até setembro de 2014, uma proposta de base jurídica para as atividades do Centro da UE para a Análise de Informações (IntCen), assim como um mecanismo de controlo adequado adaptado às suas atividades, incluindo a comunicação regular de informações ao Parlamento Europeu;

70. Insta a Comissão a apresentar, até setembro de 2014, uma proposta de um procedimento de autorização de segurança da UE para todos os titulares de cargos públicos da UE, uma vez que o atual sistema, que depende da autorização de segurança emitida pelo Estado-Membro do titular, prevê requisitos diferentes e procedimentos com durações diferentes nos vários sistemas nacionais, levando a um tratamento desigual dos eurodeputados e do respetivo pessoal consoante a sua nacionalidade;

71. Recorda as disposições do Acordo Interinstitucional entre o Parlamento Europeu e o Conselho sobre o envio ao Parlamento Europeu e o tratamento, por parte deste, de informações classificadas na posse do Conselho relativas a matérias não abrangidas pela Política Externa e de Segurança Comum, que deveriam ser utilizadas para

[1] «The Global Principles on National Security and the Right to Information», junho de 2013.

melhorar o controlo a nível da UE;

Agências da UE

72. Solicita à Instância Comum de Controlo da Europol, juntamente com as autoridades nacionais de proteção dos dados, que realize uma inspeção conjunta antes do final de 2014 a fim de determinar se as informações e os dados pessoais partilhados com a Europol foram adquiridos legalmente pelas autoridades nacionais, em particular se as informações ou dados foram inicialmente adquiridos por serviços de informação na UE ou num país terceiro, e se estão em vigor medidas apropriadas para prevenir a utilização e a divulgação dessas informações ou dados;

73. Insta a Europol a solicitar às autoridades competentes dos Estados-Membros, em consonância com as suas competências, que iniciem inquéritos sobre possíveis cibercrimes e ciberataques cometidos por governos ou intervenientes privados no decurso das atividades em análise;

Liberdade de expressão

74. Manifesta profunda preocupação com as crescentes ameaças à liberdade de imprensa e com o efeito assustador, para os jornalistas, da intimidação pelas autoridades estatais, em particular no que diz respeito à proteção da confidencialidade das fontes jornalísticas; reitera os apelos manifestados na sua Resolução, de 21 de maio de 2013, sobre a Carta da UE: enquadramento geral da liberdade nos meios de comunicação social na UE;

75. Considera que a detenção de David Miranda e a apreensão do material que se encontrava na sua posse ao abrigo do Apêndice 7 do Terrorism Act 2000 (e também o pedido ao *The Guardian* para que destruísse ou entregasse o material) constitui uma interferência com o direito à liberdade de expressão consagrado no artigo 10.º da CEDH e no artigo 11.º da Carta da UE;

76. Insta a Comissão a apresentar uma proposta de um quadro abrangente para a proteção de denunciantes na UE, com especial atenção às especificidades da denúncia no domínio dos serviços de informação, para a qual as disposições relativas à denúncia no domínio financeiro podem ser insuficientes, e incluindo fortes garantias de imunidade;

Segurança informática na UE

77. Salienta que os recentes incidentes demonstram claramente a enorme vulnerabilidade da UE, e em particular das instituições da UE, dos governos e parlamentos nacionais, das principais empresas europeias e das infraestruturas e redes informáticas europeias, a ataques sofisticados utilizando *software* complexo; observa que estes ataques requerem recursos financeiros e humanos de tal ordem que é altamente provável que tenham origem em entidades públicas que atuam em nome de governos estrangeiros, ou até em certos governos nacionais da UE que os apoiam; neste contexto, observa o caso de intrusão ou instalação de dispositivos de interceção na empresa de telecomunicações Belgacom como um exemplo preocupante de um ataque contra a capacidade informática da UE;

78. Considera que as revelações de vigilância em larga escala que iniciaram esta crise podem ser utilizadas como uma oportunidade para a Europa tomar a iniciativa de desenvolver uma capacidade autónoma de recursos informáticos fundamentais a médio prazo; insta a Comissão e os Estados-Membros a recorrerem à contratação pública como impulso para apoiar essa capacidade de recursos na UE tornando as normas de segurança e privacidade da UE num requisito de base para os contratos públicos de bens e serviços de informática;

79. Está seriamente preocupado com as indicações de que os serviços de informação estrangeiros procuraram reduzir as normas de segurança informática e instalar funções-alçapão num vasto conjunto de sistemas informáticos;

80. Insta todos os Estados-Membros, a Comissão, o Conselho e o Conselho Europeu a abordarem a perigosa falta de autonomia da UE em termos de ferramentas, empresas e prestadores de serviços de informática (*hardware*, *software*, serviços e redes), assim como de capacidades de encriptação e criptografia;

81. Insta a Comissão, os organismos de normalização e a ENISA a desenvolverem, até setembro de 2014, normas e orientações mínimas de segurança e privacidade para os sistemas, redes e serviços informáticos, incluindo serviços de computação em nuvem, a fim de proteger melhor os dados pessoais dos cidadãos da UE; considera que estas normas deveriam ser definidas mediante um processo aberto e democrático e não conduzido por um único país, entidade ou empresa multinacional; entende que, apesar de deverem ser tidas em conta no apoio à luta contra o terrorismo, as preocupações legítimas em matéria de aplicação da lei e informação não devem levar a um compromisso generalizado da fiabilidade de todos os sistemas informáticos;

82. Salienta que tanto as empresas de telecomunicações como os reguladores de telecomunicações nacionais e da UE têm negligenciado claramente a segurança informática dos seus utilizadores e clientes; insta a Comissão a exercer plenamente as suas competências decorrentes da Diretiva-Quadro Privacidade e Comunicações Eletrónicas para reforçar a proteção da confidencialidade das comunicações adotando medidas destinadas a garantir que o equipamento terminal é compatível com o direito dos utilizadores ao controlo e à proteção dos seus dados pessoais e a assegurar um elevado nível de segurança das redes e serviços de telecomunicações, nomeadamente através da exigência de uma encriptação sofisticada das comunicações;

83. Apoia a estratégia de segurança cibernética da UE, mas considera que esta não abrange todas as ameaças possíveis e que deveria ser alargada de forma a abranger comportamentos maliciosos do Estado;

84. Insta a Comissão, o mais tardar até janeiro de 2015, a apresentar um Plano de Ação para o desenvolvimento de uma maior independência da UE no setor da informática, incluindo uma abordagem mais coerente ao impulsionamento das capacidades de tecnologia informática europeias (incluindo sistemas, equipamentos e serviços informáticos, computação em nuvem, encriptação e anonimização) e à proteção da infraestrutura informática crítica (nomeadamente em termos de propriedade e vulnerabilidade);

85. Apela à Comissão, no contexto do próximo Programa de Trabalho sobre o Horizonte 2020, que avalie se deveriam ser dedicados mais recursos ao impulsionamento da investigação, do desenvolvimento, da inovação e da formação europeus no domínio das tecnologias da informação, em particular das tecnologias e infraestruturas de reforço da privacidade, da criptologia, da computação segura, das soluções seguras de fonte aberta e da Sociedade da Informação;

86. Solicita à Comissão que defina as atuais responsabilidades e que reveja, o mais tardar até junho de 2014, a necessidade de um mandato mais amplo, de uma melhor coordenação e/ou de recursos e capacidades técnicas adicionais para o centro de cibercriminalidade da Europol, a ENISA, a CERT-UE e a AEPD a fim de lhes permitir serem mais eficazes na investigação de violações informáticas graves na UE e no desempenho (ou na assistência aos Estados-Membros e aos órgãos da UE) de investigações técnicas no local relativas a violações informáticas graves;

87. Considera necessário que a UE seja apoiada por uma Academia de Informática da UE que reúna os melhores peritos europeus em todos os domínios conexos, encarregados de prestar, a todas as instituições e órgãos da UE, aconselhamento científico sobre tecnologias da informação, incluindo estratégias relacionadas com a segurança; solicita à Comissão, em primeiro lugar, que crie um painel de peritos científicos independentes;

88. Insta o Secretariado do Parlamento Europeu a realizar, o mais tardar até setembro de 2014, uma revisão e uma avaliação aprofundadas da fiabilidade da segurança informática do Parlamento Europeu, centrando-se em: recursos orçamentais, recursos humanos, capacidades técnicas, organização interna e todos os elementos pertinentes, com vista a alcançar um elevado nível de segurança para os sistemas de informática da UE; considera que uma tal avaliação deveria fornecer, pelo menos, uma análise da informação e recomendações sobre:

- A necessidade de auditorias regulares, rigorosas e independentes à segurança, assim como de testes de penetração, com a seleção de peritos em segurança externos, assegurando a transparência e a garantia de credenciais relativamente a países terceiros ou qualquer tipo de interesses próprios;

- A inclusão, nos procedimentos de concurso para novos sistemas informáticos, de requisitos específicos em matéria de segurança/privacidade informática, incluindo a possibilidade de um requisito de *software* de fonte aberta como condição de compra;

- A lista das empresas dos EUA com contratos com o Parlamento Europeu nos domínios da informática e das telecomunicações, tendo em conta as revelações sobre os contratos da NSA com uma empresa como a RSA, cujos produtos o Parlamento Europeu utiliza para, presumivelmente, proteger o acesso à distância aos seus dados pelos seus membros e pessoal;

- A fiabilidade e a resistência de *software* comercial de terceiros utilizado pelas instituições da UE nos seus sistemas informáticos relativamente a penetrações

e intrusões por autoridades de aplicação da lei e de informação da UE ou de países terceiros;

- A utilização de mais sistemas de fonte aberta e de menos sistemas comerciais disponíveis no mercado;

- O impacto do aumento da utilização de dispositivos móveis (*smartphones*, *tablets*, profissionais ou pessoais) e os seus efeitos na segurança informática do sistema;

- A segurança das comunicações entre diferentes locais de trabalho do Parlamento Europeu e dos sistemas informáticos utilizados no Parlamento Europeu;

- A utilização e localização de servidores e centros de informática dos sistemas informáticos do PE e as suas implicações para a segurança e a integridade dos sistemas;

- A aplicação efetiva das regras em vigor sobre violações da segurança e a notificação imediata das autoridades competentes pelos prestadores de redes de telecomunicações disponíveis ao público;

- A utilização da armazenagem em nuvem pelo PE, incluindo o tipo de dados armazenados em nuvem, a forma como os conteúdos e o acesso aos mesmos são protegidos e a localização da nuvem, clarificando o regime jurídico de proteção de dados aplicável;

- Um plano que permita a utilização de mais tecnologias criptográficas, em particular a encriptação autenticada extremo a extremo de todos os serviços de informática e comunicações, como computação em nuvem, correio eletrónico, mensagens instantâneas e telefonia;

- A utilização de assinatura eletrónica no correio eletrónico;

- Uma análise dos benefícios da utilização do GNU Privacy Guard como norma de encriptação predefinida para correio eletrónico, que permitiria, ao mesmo tempo, a utilização de assinaturas digitais;

- A possibilidade de criar um serviço seguro de mensagens instantâneas no Parlamento Europeu que permita comunicações seguras, em que o servidor apenas teria acesso a conteúdo encriptado;

89. Insta todas as instituições e agências da UE a realizarem um exercício semelhante, o mais tardar até dezembro de 2014, em particular o Conselho Europeu, o Conselho, o Serviço Europeu de Ação Externa (incluindo as delegações da UE), a Comissão, o Tribunal de Justiça e o Banco Central Europeu; convida os Estados-Membros a realizarem avaliações similares;

90. Salienta que, no que diz respeito à ação externa da UE, devem ser realizadas

avaliações das necessidades orçamentais relacionadas e devem ser tomadas medidas de imediato no caso do Serviço Europeu de Ação Externa (SEAE), tendo de ser atribuídos fundos apropriados no Projeto de Orçamento para 2015;

91. Considera que os sistemas informáticos a larga escala utilizados no domínio da liberdade, da segurança e da justiça, como o Sistema de Informação Schengen II, o Sistema de Informação sobre Vistos, o Eurodac, assim como possíveis futuros sistemas, deveriam ser desenvolvidos e operados de forma a garantir que os dados não sejam comprometidos na sequência de pedidos dos EUA ao abrigo do Patriot Act; solicita à eu-LISA que comunique ao Parlamento informações sobre a fiabilidade dos sistemas em vigor até ao final de 2014;

92. Insta a Comissão e o SEAE a tomarem medidas a nível internacional, em particular com a ONU e em cooperação com parceiros interessados (como o Brasil) e a implementarem uma estratégia da UE para a governação democrática da Internet destinada a prevenir influências indevidas sobre as atividades da ICANN e da IANA por entidades, empresas ou países, garantindo uma representação adequada de todas as partes interessadas nestes órgãos;

93. Apela à reconsideração da arquitetura global da Internet em termos de fluxos e armazenamento de dados, defendendo uma maior minimização e transparência de dados e um menor armazenamento em larga escala centralizado de dados brutos, assim como evitando um encaminhamento desnecessário de tráfego através do território de países que não cumpram as normas básicas em matéria de direitos fundamentais, proteção de dados e privacidade;

94. Insta os Estados-Membros, em cooperação com a ENISA, o centro de cibercriminalidade da Europol, as CERT, as autoridades nacionais de proteção de dados e as unidades de luta contra a cibercriminalidade, a iniciarem uma campanha de educação e consciencialização destinada a permitir que os cidadãos façam uma escolha mais informada relativamente aos dados pessoais que colocam em linha e à melhor forma de os proteger, incluindo através da «higiene digital», da encriptação e da computação em nuvem segura, fazendo pleno uso da plataforma de informação de interesse público prevista na Diretiva Serviço Universal;

95. Insta a Comissão, até setembro de 2014, a avaliar as possibilidades de incentivar os fabricantes de *software* e *hardware* a introduzirem uma maior segurança e privacidade através de funcionalidades predefinidas nos seus produtos, incluindo a possibilidade de introduzir responsabilidade jurídica da parte dos fabricantes para vulnerabilidades conhecidas não corrigidas ou a instalação de funções-alçapão secretas, bem como desincentivos à recolha indevida e desproporcionada de dados pessoais em massa, e, se apropriado, a apresentar propostas legislativas;

Restabelecer a confiança

96. Acredita que o inquérito demonstrou a necessidade de os EUA restabelecerem a confiança com os seus parceiros, uma vez que estão em causa sobretudo as atividades das agências de informação norte-americanas;

97. Salienta que a crise de confiança que se gerou se estende:

– Ao espírito de cooperação com a UE, uma vez que algumas atividades de informação a nível nacional podem por em perigo a consecução dos objetivos da União;

– Aos cidadãos, que se aperceberam de que, não só países terceiros ou empresas multinacionais, mas também o seu próprio governo, os pode estar a espiar;

– Ao respeito pelo Estado de direito e à credibilidade das garantias democráticas numa sociedade digital;

Entre a UE e os EUA

98. Recorda a importante parceria histórica e estratégica entre os Estados-Membros da UE e os EUA, baseada numa convicção comum na democracia, no Estado de direito e nos direitos fundamentais;

99. Considera que a vigilância em larga escala dos cidadãos e a espionagem dos líderes políticos pelos EUA causaram danos graves às relações entre a UE e os EUA e prejudicaram a confiança nas organizações norte-americanas que atuam na UE; tal é ainda mais agravado pela falta de direitos a recurso judicial e administrativo da legislação americana para os cidadãos da UE, particularmente em casos de atividades de vigilância para efeitos de informação;

100. Reconhece, à luz dos desafios globais que a UE e os EUA enfrentam, que a parceria transatlântica tem de ser mais reforçada, e que é fundamental que a cooperação transatlântica na luta contra o terrorismo prossiga; insiste, contudo, que os EUA têm de tomar medidas claras para restabelecer a confiança e volta a enfatizar os valores básicos partilhados subjacentes à parceria;

101. Está preparado para participar ativamente num diálogo com os seus homólogos norte-americanos para que, no debate em curso nos EUA a nível público e do Congresso sobre a reforma da vigilância e a revisão do controlo da informação, os direitos dos cidadãos da UE à vida privada sejam abordados, para que sejam garantidos direitos iguais à informação e à proteção da privacidade nos tribunais norte-americanos e para que a atual discriminação não seja perpetuada;

102. Insiste que têm de ser levadas a cabo reformas e instituídas garantias eficazes para os europeus para assegurar que a utilização da vigilância e do tratamento de dados para os serviços de informação externos seja limitada por condições claramente especificadas e relacionadas com suspeitas razoáveis ou causa provável de atividade terrorista ou criminosa; salienta que este objetivo deve estar sujeito a controlo judicial transparente;

103. Considera que são necessários sinais políticos claros dos nossos parceiros americanos que demonstrem que os EUA fazem uma distinção entre aliados e adversários;

104. Exorta a Comissão Europeia e a Administração dos EUA a abordarem, no contexto

das negociações em curso sobre um acordo global UE-EUA sobre a transferência de dados para efeitos de aplicação da lei, os direitos dos cidadãos da UE à informação e a recurso judicial, bem como a concluírem estas negociações, em consonância com o compromisso feito na reunião ministerial «Justiça e Assuntos Internos» UE-EUA, de 18 de novembro de 2013, antes do verão de 2014;

105. Incentiva os EUA a aderirem à Convenção do Conselho da Europa para a Proteção das Pessoas no que respeita ao Processamento Automático de Dados Pessoais (Convenção n.º 108), tal como aderiram à Convenção sobre a Cibercriminalidade em 2001, reforçando a base jurídica partilhada pelos aliados transatlânticos;

106. Insta as instituições da UE a explorarem a possibilidade de estabelecer, com os EUA, um código de conduta que garanta que não é empreendida espionagem dos EUA contra instituições e instalações da UE;

Dentro da União Europeia

107. Entende, além disso, que o envolvimento e as atividades dos Estados-Membros da UE levaram a uma perda da confiança; considera que apenas a clareza total relativamente aos fins e aos meios de vigilância, o debate público e, em última instância, a revisão da legislação, incluindo um reforço do sistema de controlo judicial e parlamentar, serão capazes de restabelecer a confiança perdida;

108. Está ciente de que alguns Estados-Membros da UE se encontram em comunicações bilaterais com as autoridades norte-americanas sobre alegações de espionagem, e que alguns deles celebraram (Reino Unido) ou preveem a celebração (Alemanha, França) de chamados acordos «anti-espionagem»; sublinha que estes Estados-Membros têm de observar plenamente os interesses da UE enquanto um todo;

109. Considera que estes acordos não deverão violar os Tratados europeus, principalmente o princípio da cooperação leal (nos termos do artigo 4.º, n.º 3, do TUE) ou comprometer as políticas da UE em geral e, mais especificamente, o mercado interno, a concorrência leal e o desenvolvimento económico, industrial e social; reserva-se o direito de ativar os procedimentos do Tratado caso tais acordos se revelem contrários à coesão da União ou aos princípios fundamentais nos quais esta assenta;

A nível internacional

110. Insta a Comissão a apresentar, o mais tardar em janeiro de 2015, uma estratégia da UE para a governação democrática da Internet;

111. Convida os Estados-Membros a darem seguimento ao apelo da 35.ª Conferência Internacional de Proteção de Dados e Responsáveis pela Privacidade de «defender a adoção de um protocolo adicional ao artigo 17.º do Pacto Internacional sobre Direitos Civis e Políticos (PIDCP), que deverá assentar nas normas que foram desenvolvidas e subscritas pela Conferência Internacional e nas disposições da observação de caráter geral n.º 16 ao Pacto, a fim de criar normas globalmente aplicáveis em matéria de proteção de dados e a proteção da privacidade em conformidade com o Estado de direito»; solicita à Alta Representante/Vice-Presidente da Comissão e do Serviço

Europeu de Ação Externa que assuma uma postura pró-ativa;

112. Insta os Estados-Membros a desenvolverem uma estratégia coerente e sólida no âmbito das Nações Unidas, apoiando em particular a resolução sobre «O direito à privacidade na era digital» iniciada pelo Brasil e pela Alemanha e adotada pela Comissão da Assembleia Geral da ONU (Comissão dos Direitos do Homem) em 27 de novembro de 2013;

Plano de prioridades: um Habeas Corpus Digital Europeu

113. Decide apresentar aos cidadãos, às instituições e aos Estados-Membros da UE as recomendações supramencionadas sob a forma de um Plano de prioridades para a próxima legislatura;

114. Decide lançar um *Habeas Corpus* Digital Europeu para proteger a privacidade baseado nas seguintes 7 ações sob a supervisão do Parlamento Europeu:

Ação 1: adotar o pacote relativo à proteção de dados em 2014;

Ação 2: celebrar o acordo global UE-EUA, garantindo mecanismos adequados de recurso para os cidadãos da UE em caso de transferências de dados da UE para os EUA para efeitos de aplicação da lei;

Ação 3: suspender o «porto seguro» até que tenha sido realizada uma revisão aprofundada e colmatadas as lacunas, garantindo que as transferências de dados para fins comerciais da União para os EUA apenas podem ser realizadas em conformidade com as mais elevadas normas da UE;

Ação 4: suspender o Acordo TFTP até que (i) tenham sido concluídas as negociações sobre o acordo global; (ii) tenha sido concluído um inquérito aprofundado com base numa análise da UE, e todas as preocupações levantadas pelo Parlamento na sua Resolução de 23 de outubro tenham sido devidamente abordadas;

Ação 5: proteger o Estado de direito e os direitos fundamentais dos cidadãos da UE, com atenção particular às ameaças à liberdade de imprensa e à confidencialidade profissional (incluindo relações advogado-cliente), assim como ao reforço da proteção dos denunciantes;

Ação 6: desenvolver uma estratégia europeia para a independência informática (a nível nacional e da UE);

Ação 7: desenvolver a UE como interveniente de referência na governação democrática e neutra da Internet;

115. Insta as instituições e os Estados-Membros da UE a apoiarem e promoverem o *Habeas Corpus* Digital Europeu; compromete-se a agir como guardião dos direitos dos cidadãos da UE, cumprindo o seguinte calendário de acompanhamento da execução:

- Abril-julho de 2014: um grupo de acompanhamento baseado na equipa de inquérito da LIBE responsável pelo acompanhamento de novas revelações nos meios de comunicação social relativas ao mandato de inquérito e pelo escrutínio da execução desta resolução;

- A partir de julho de 2014: um mecanismo permanente de controlo para transferências de dados e recursos judiciais junto da comissão competente;

- Primavera de 2014: um apelo formal ao Conselho Europeu para incluir o *Habeas Corpus* Digital Europeu nas orientações a adotar ao abrigo do artigo 68.º do TFUE;

- Outono de 2014: um compromisso de que o *Habeas Corpus* Digital Europeu e as recomendações conexas servirão de critérios de base para a aprovação da próxima Comissão;

- 2014-2015: um grupo de Confiança/Dados/Direitos dos Cidadãos que reúna regularmente entre o Parlamento Europeu e o Congresso dos EUA, assim como com outros parlamentos de países terceiros empenhados, incluindo o Brasil;

- 2014-2015: uma conferência com as entidades de controlo dos serviços de informação dos parlamentos nacionais europeus;

- 2015: uma conferência que reúna peritos europeus de alto nível nos vários domínios conducentes à segurança informática (incluindo a matemática, a criptografia e as tecnologias de reforço da privacidade) destinada a ajudar a promover uma estratégia informática da UE para a próxima legislatura;

116. Encarrega o seu Presidente de transmitir a presente Resolução ao Conselho Europeu, ao Conselho, à Comissão, aos parlamentos e governos dos Estados-Membros, às autoridades nacionais de proteção de dados, à AEPD, à eu-LISA, à ENISA, à Agência dos Direitos Fundamentais, ao Grupo de Trabalho do Artigo 29.º, ao Conselho da Europa, ao Congresso dos Estados Unidos da América, à Administração dos EUA, ao Presidente, ao Governo e ao Parlamento da República Federativa do Brasil e ao Secretário-Geral das Nações Unidas.

EXPOSIÇÃO DE MOTIVOS

«O cargo do soberano, seja ele um monarca ou uma assembleia, consiste no objetivo para o qual lhe foi confiado o soberano poder, nomeadamente a obtenção da segurança do povo»
Hobbes, Leviatã (capítulo XXX)

«Não podemos louvar, perante os outros, a nossa sociedade afastando-nos dos padrões fundamentais que a tornam digna de louvor»
Lord Bingham of Cornhill,
Antigo Presidente do Supremo Tribunal de Inglaterra e do País de Gales

Metodologia

A partir de julho de 2013, a Comissão de Inquérito LIBE foi responsável pela tarefa extremamente difícil de cumprir o mandato[1] do Plenário de investigar a vigilância eletrónica em larga escala dos cidadãos da UE num prazo muito curto, de menos de 6 meses.

Durante esse período, realizou mais de 15 audições, abrangendo cada uma das questões centrais previstas na Resolução de 4 de julho, baseando-se nas propostas de peritos da UE e dos EUA, que representavam um vasto conjunto de conhecimentos e contextos: as instituições da UE, os parlamentos nacionais, o Congresso dos EUA, académicos, jornalistas, a sociedade civil, especialistas em segurança e tecnologia e empresas privadas. Além disso, uma delegação da Comissão LIBE visitou Washington em 28-31 de outubro de 2013 para reunir com representantes dos ramos executivo e legislativo (académicos, advogados, especialistas em segurança, representantes de empresas)[2]. Uma delegação da Comissão dos Assuntos Externos (AFET) esteve na cidade ao mesmo tempo. Realizaram-se algumas reuniões com ambas as delegações.

Uma série de documentos de trabalho[3] foram corredigidos pelo relator, pelos relatores-sombra[4] dos vários grupos políticos e por três membros da Comissão AFET[5] permitindo uma apresentação das principais conclusões do inquérito. O relator gostaria de agradecer a todos os relatores-sombra, bem como aos membros da AFET, pela sua cooperação próxima e pelo elevado nível de empenho ao longo deste exigente processo.

Dimensão do problema

A atenção crescente à segurança, aliada à evolução tecnológica, permitiu aos Estados

[1] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_pt.pdf
[2] Ver o relatório da delegação a Washington.
[3] Ver anexo I.
[4] Lista de relatores-sombra: Axel Voss (PPE), Sophia in't Veld (ALDE), Jan Philipp Albrecht (Verts/ALE), Timothy Kirkhope (EFD), Cornelia Ernst (GUE).
[5] Lista de membros da AFET: José Ignacio Salafranca Sánchez-Neyra (PPE), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).

saber mais do que nunca sobre os cidadãos. A possibilidade de recolher dados relativos ao conteúdo das comunicações, bem como metadados, e de seguir as atividades eletrónicas dos cidadãos – em particular, a sua utilização de *smartphones* e computadores *tablet* – faz com que os serviços de informações possam, efetivamente, saber quase tudo sobre uma pessoa. Tudo isto **contribuiu para uma transição fundamental no trabalho e nas práticas das agências de informação, afastando-se do conceito tradicional de vigilância orientada como medida contra o terrorismo necessária e proporcional, rumo a sistemas de vigilância em larga escala**.

Este processo de vigilância em larga escala crescente ainda não tinha sido sujeito a qualquer debate público ou processo de decisão democrática. É necessário debater o objetivo e a dimensão da vigilância e o seu lugar numa sociedade democrática. Será a situação criada pelas revelações de Edward Snowden uma indicação de uma viragem societal geral para a aceitação da morte da privacidade em troca da segurança? Estaremos perante uma violação da privacidade e da intimidade de tal ordem que é possível, não só para os criminosos mas também para as empresas de informática e para as agências de informação, conhecer tudo sobre a vida de um cidadão? Será este um facto a aceitar sem mais discussão? Ou será da responsabilidade do legislador adaptar os instrumentos políticos e jurídicos existentes de forma a limitar os riscos e prevenir mais prejuízos no caso de chegarem ao poder forças menos democráticas?

Reações à vigilância em larga escala e debate público

O debate sobre a vigilância em larga escala não tem lugar de forma homogénea dentro da UE. Na verdade, em muitos Estados-Membros não existe praticamente qualquer debate público, e a atenção dos meios de comunicação social é heterogénea. A Alemanha parece ser o país onde se observaram reações mais fortes às revelações e onde os debates públicos sobre as suas consequências se generalizaram. No Reino Unido e em França, apesar dos inquéritos realizados pelo *The Guardian* e o *Le Monde*, as reações parecem mais limitadas, um facto que tem sido associado ao alegado envolvimento dos seus serviços nacionais de informação em atividades com a NSA. O Inquérito da Comissão LIBE esteve em posição de ouvir contribuições valiosas das entidades de controlo parlamentar da Bélgica, dos Países Baixos, da Dinamarca e até da Noruega; no entanto, o parlamento britânico e o parlamento francês declinaram o convite à participação. Estas diferenças demonstram, uma vez mais, o grau de desigualdade dos controlos e equilíbrios, na UE, sobre estas questões, salientando que é necessário uma maior cooperação entre os órgãos parlamentares responsáveis pelo controlo.

Após as revelações de Edward Snowden nos meios de comunicação de massas, o debate público tem-se baseado em dois tipos principais de reações. Por um lado, os que negam a legitimidade das informações publicadas alegando que a maior parte das reportagens dos meios de comunicação social se baseia em interpretações erróneas; além disso, muitos questionam, sem contudo refutarem as revelações, a validade das divulgações devido aos alegados riscos de segurança que implicam a nível da segurança nacional e da luta contra o terrorismo.

Por outro lado, existem os que consideram que as informações divulgadas requerem um debate público e informado, devido à magnitude do problema que levantam no que diz respeito a questões que são fundamentais para a democracia, incluindo: o Estado de direito, os

direitos fundamentais, a privacidade dos cidadãos, a responsabilidade pública dos serviços de aplicação da lei e de informação, etc. Este é o caso, certamente, dos jornalistas e editores das principais agências de notícias do mundo que têm acesso às divulgações, incluindo o *The Guardian*, o *Le Monde*, o *Der Spiegel*, o *The Washington Post* e Glenn Greenwald.

Os dois tipos de reações supramencionados baseiam-se num conjunto de motivos que, se seguidos, podem levar a decisões bastante opostas sobre como a UE deve ou não reagir.

Cinco motivos para não agir

– *O argumento «serviços de informação/segurança nacional»: ausência de competência da UE*

As revelações de Edward Snowden estão relacionadas com os EUA e atividades de informação de alguns Estados-Membros, no entanto a segurança nacional é uma competência nacional, pelo que a UE não possui competência nesta matéria (salvo no que diz respeito à segurança interna da UE), não sendo possível qualquer ação a nível da UE.

– *O argumento «terrorismo»: perigo para o denunciante*

Qualquer seguimento dado a estas revelações, ou a sua mera consideração, fragiliza ainda mais a segurança dos EUA e da UE, uma vez que não condena a publicação de documentos cujo conteúdo, mesmo que tenha sido redigido conforme explicado pelos intervenientes dos meios de comunicação envolvidos, pode facultar informações valiosas a grupos terroristas.

– *O argumento «traição»: ausência de legitimidade do denunciante*

Tal como avançado principalmente por entidades nos EUA e no Reino Unido, qualquer debate lançado ou ação prevista na sequência das revelações de E. Snowden é intrinsecamente parcial e irrelevante, uma vez que se baseia num ato inicial de traição.

– *O argumento «realismo»: interesses estratégicos gerais*

Mesmo que alguns erros e atividades ilegais fossem confirmados, deveriam ser contrabalançados com a necessidade de conservar a relação especial entre os EUA e a Europa a fim de preservar os interesses partilhados a nível económico, empresarial e de política externa.

– *O argumento «boa governação»: confia no teu governo*

Os governos dos EUA e da UE são democraticamente eleitos. No domínio da segurança, e mesmo quando são levadas a cabo atividades de informação com vista à luta contra o terrorismo, estes cumprem, por princípio, normas democráticas. Esta «presunção de uma governação boa e legítima» assenta, não só na boa vontade dos titulares dos poderes executivos nestes Estados, como também no mecanismo de controlos e equilíbrios consagrado nos seus sistemas constitucionais.

Como se pode constatar, são muitos e poderosos os motivos para não agir. Estes motivos

podem explicar porque é que a maioria dos governos da UE, após algumas reações fortes iniciais, preferiram não agir. A principal ação do Conselho de Ministros foi a criação de um «grupo transatlântico de peritos em proteção de dados», que reuniu três vezes e apresentou um relatório final. Pressupõe-se que um segundo grupo de autoridades dos EUA e dos Estados-Membros terá reunido sobre questões relacionadas com os serviços de informação, mas não existem informações disponíveis sobre tal reunião. O Conselho Europeu abordou o problema da vigilância numa declaração de Chefes de Estado e de Governo[1]. Até agora, apenas alguns parlamentos nacionais lançaram inquéritos.

Cinco motivos para agir

– *O argumento «vigilância em larga escala»: em que sociedade queremos viver?*

Desde a primeira revelação, em junho de 2013, que têm sido feitas referências consistentes à obra *1984* de George Orwell. Desde os ataques de 11 de setembro de 2001, a atenção à segurança e a passagem para uma vigilância focada e específica prejudicou e comprometeu gravemente o conceito de privacidade. A história da Europa e dos EUA evidencia os perigos da vigilância em larga escala e da passagem gradual para sociedades sem privacidade.

– *O argumento «direitos fundamentais»:*

A vigilância em larga escala e indiscriminada põe em causa os direitos fundamentais dos cidadãos, incluindo o direito à privacidade, à proteção de dados, à liberdade de imprensa e a um tribunal imparcial, todos eles consagrados nos Tratados da UE, na Carta dos Direitos Fundamentais e na CEDH. Estes direitos não podem ser contornados nem negociados em troca de possíveis benefícios, a menos que tal seja devidamente previsto em instrumentos jurídicos e em plena conformidade com os Tratados.

– O argumento «segurança interna da UE»:

A competência nacional em matéria de informação e segurança nacional não exclui uma competência paralela da UE. A UE tem exercido as competências que lhe são atribuídas pelos Tratados da UE em matéria de segurança interna decidindo quanto a uma série de instrumentos legislativos e celebrando acordos internacionais destinados a combater os crimes graves e o terrorismo, bem como criando uma estratégia de segurança interna e agências para operar neste domínio. Além disso, foram desenvolvidos outros serviços que refletem a necessidade de uma maior cooperação a nível da UE em matéria de informação: o INTCEN (que faz parte do SEAE) e o Coordenador da Luta Antiterrorista (que faz parte do Secretariado-Geral do Conselho), nenhum deles com base jurídica.

– *O argumento «controlo insuficiente»:*

[1] Conclusões do Conselho Europeu, de 24-25 de outubro de 2013, em particular: «Os Chefes de Estado e de Governo tomaram nota da intenção da França e da Alemanha de procurar conversações bilaterais com os EUA com vista a chegar, antes do final do ano, a um entendimento sobre relações mútuas nesse domínio. Salientaram que outros países da UE são convidados a aderir à iniciativa. Destacaram ainda o Grupo de Trabalho existente entre a UE e os EUA sobre a questão conexa da proteção de dados e apelaram a um progresso rápido e construtivo nesse sentido».

Apesar de desempenharem um papel indispensável na proteção contra ameaças internas e externas, os serviços de informação têm de operar no âmbito do Estado de direito e, para tal, devem estar sujeitos a um mecanismo de controlo rigoroso e abrangente. O controlo democrático das atividades de informação é realizado a nível nacional. No entanto, devido à natureza internacional das ameaças de segurança, existe agora um enorme intercâmbio de informações entre os Estados-Membros e com países terceiros como os EUA; são necessárias melhorias nos mecanismos de controlo, tanto a nível nacional como da UE, a fim de evitar que os mecanismos de controlo tradicionais se tornem ineficazes e obsoletos.

– *O «efeito assustador para os meios de comunicação social» e a proteção dos denunciantes*

As revelações de Edward Snowden e as posteriores reportagens dos meios de comunicação social sublinharam o papel central dos meios de comunicação numa democracia para garantia a responsabilização dos governos. Quando os mecanismos de controlo são incapazes de prevenir ou retificar a vigilância em larga escala, o papel dos meios de comunicação social e dos denunciantes na revelação de eventuais ilegalidades ou abusos de poder é extremamente importante. As reações das autoridades dos EUA e do Reino Unido aos meios de comunicação social revelaram a vulnerabilidade da imprensa e dos denunciantes e a necessidade urgente de os proteger melhor.

A União Europeia é obrigada a escolher entre uma política de «manter a situação atual» (motivos suficientes para não agir, esperar para ver) e uma política de «aceitar a realidade» (a vigilância não é uma situação nova, mas existem provas suficientes de uma magnitude sem precedentes do alcance e das capacidades das agências de informação que obrigam a UE a agir).

Habeas corpus numa sociedade da vigilância

Em 1679, o parlamento britânico adotou o Habeas Corpus Act como um passo determinante no sentido da garantia do direito a um juiz numa altura de rivalidade entre jurisdições e conflitos de leis. Atualmente, as nossas democracias garantem direitos adequados para condenados ou detidos que são fisicamente sujeitos a um processo penal ou levados a tribunal. No entanto, os seus dados, que são inseridos, tratados, armazenados e localizados em redes digitais, formam um «corpo de dados pessoais», uma espécie de corpo digital específico para cada indivíduo e que permite revelar grande parte da sua identidade, hábitos e preferências de todo o tipo.

O Habeas Corpus é reconhecido como um instrumento jurídico fundamental para salvaguardar a liberdade individual contra ação arbitrária do Estado. O que é necessário hoje é uma extensão do Habeas Corpus à era digital. Estão em causa o direito à privacidade e o respeito pela integridade e pela dignidade do indivíduo. As recolhas em larga escala de dados sem respeito pelas normas da UE em matéria de proteção de dados e as violações específicas do princípio da proporcionalidade na gestão de dados são contrários às tradições constitucionais dos Estados-Membros e aos fundamentos da ordem constitucional europeia.

A principal novidade hoje é que estes riscos não têm apenas origem em atividades criminosas (contra as quais o legislador da UE adotou uma série de instrumentos) ou em possíveis ciberataques de governos de países com um fraco historial democrático. Estamos a

aperceber-nos de que estes riscos podem advir também de serviços de aplicação da lei e informação de países democráticos, que colocam os cidadãos ou as empresas da UE sob conflitos de leis, resultando num enfraquecimento da certeza jurídica, com possíveis violações de direitos sem que existam mecanismos adequados de reparação.

É necessária uma governação das redes para garantir a segurança dos dados pessoais. Antes do desenvolvimento dos Estados modernos, não era possível garantir a segurança nas ruas ou nas estradas e a integridade física dos cidadãos estava em risco. Hoje, apesar de dominarem a vida quotidiana, as autoestradas da informação não são seguras. A integridade dos dados digitais deve ser assegurada, contra criminosos, evidentemente, mas também contra possíveis abusos de poder pelas autoridades ou colaboradores do Estado e por empresas privadas ao abrigo de mandados judiciais secretos.

Recomendações do Inquérito da Comissão LIBE

Muitos dos problemas levantados hoje são extremamente semelhantes aos revelados pelo Inquérito do Parlamento Europeu relativo ao programa Echelon em 2001. A impossibilidade da legislatura anterior acompanhar as constatações e recomendações do Inquérito Echelon deveria servir de lição para este Inquérito. É por este motivo que a presente Resolução, reconhecendo a magnitude das revelações envolvidas e a sua natureza contínua, planeia tendo em vista o futuro e garante que estão na mesa propostas específicas para ações de acompanhamento na próxima legislatura, garantindo que as conclusões continuarão a ser prioritárias na agenda política da UE.

Com base nesta avaliação, o relator gostaria de submeter a votação do Parlamento as seguintes medidas:

Um *Habeas Corpus* Digital Europeu para proteger a privacidade com base em 7 ações:

Ação 1: adotar o pacote relativo à proteção de dados em 2014;

Ação 2: celebrar o acordo global UE-EUA, garantindo mecanismos adequados de recurso para os cidadãos da UE em caso de transferências de dados da UE para os EUA para efeitos de aplicação da lei;

Ação 3: suspender o «porto seguro» até que tenha sido realizada uma revisão aprofundada e tenham sido colmatadas as atuais lacunas, garantindo que as transferências de dados pessoais para fins comerciais da União para os EUA apenas podem ser realizadas em conformidade com as mais elevadas normas da UE;

Ação 4: suspender o Acordo TFTP até que (i) tenham sido concluídas as negociações sobre o acordo global; (ii) tenha sido concluído um inquérito aprofundado com base numa análise da UE, e todas as preocupações levantadas pelo Parlamento na sua Resolução de 23 de outubro tenham sido devidamente abordadas;

Ação 5: proteger o Estado de direito e os direitos fundamentais dos cidadãos da UE, com atenção particular às ameaças à liberdade de imprensa e à confidencialidade profissional (incluindo relações advogado-cliente), assim como ao reforço da

proteção dos denunciantes;

Ação 6: desenvolver uma estratégia europeia para a independência informática (a nível nacional e da UE);

Ação 7: desenvolver a qualidade da UE de interveniente de referência na governação democrática e neutra da Internet;

Após a conclusão do Inquérito, o Parlamento Europeu deverá continuar a agir como o guardião dos direitos dos cidadãos da UE, cumprindo o seguinte calendário a fim de acompanhar a execução:

- Abril-julho de 2014: um grupo de acompanhamento baseado na equipa de inquérito da LIBE responsável pelo acompanhamento de novas revelações nos meios de comunicação social relativas ao mandato de inquérito e pelo escrutínio da execução desta resolução;

- A partir de julho de 2014: um mecanismo permanente de controlo das transferências de dados e recursos judiciais no âmbito da comissão competente;

- Primavera de 2014: um apelo formal ao Conselho Europeu para incluir o *Habeas Corpus* Digital Europeu nas orientações a adotar ao abrigo do artigo 68.º do TFUE;

- Outono de 2014: um compromisso de que o *Habeas Corpus* Digital Europeu e as recomendações conexas servirão de critérios de base para a aprovação da próxima Comissão;

- 2014-2015: um grupo de Confiança/Dados/Direitos dos Cidadãos que reúna regularmente entre o Parlamento Europeu e o Congresso dos EUA, assim como com outros parlamentos de países terceiros empenhados, incluindo o Brasil;

- 2014-2015: uma conferência com as entidades europeias de controlo dos serviços de informação dos parlamentos nacionais europeus;

- 2015: uma conferência que reúna peritos europeus de alto nível nos vários domínios conducentes à segurança informática (incluindo a matemática, a criptografia e as tecnologias de reforço da privacidade) destinada a ajudar a promover uma estratégia informática da UE para a próxima legislatura;

ANEXO I: LISTA DE DOCUMENTOS DE TRABALHO

Inquérito da Comissão LIBE

Relator e relatores-sombra como coautores	Questões	Resolução do PE de 4 de julho de 2013 (ver n.ºs 15-16)
Claude Moraes (S&D)	Os programas de vigilância dos EUA e da UE e o seu impacto nos direitos fundamentais dos cidadãos da UE	N.º 16, alíneas a), b) c) e d)
Axel Voss (PPE)	**As atividades de vigilância dos EUA a respeito dos dados da UE e as suas possíveis implicações jurídicas nos acordos e na cooperação transatlânticos**	N.º 16, alíneas a), b) e c)
Sophie In't Veld (ALDE) e Cornelia Ernst (GUE)	O controlo democrático dos serviços de informações nos Estados-Membros e das agências de informações na União Europeia.	N.º 15 e n.º 16, alíneas a), c) e e)
Jan Philipp Albrecht (Verts/ALE)	A relação entre as práticas de vigilância na UE e nos EUA e as disposições em matéria de proteção de dados da UE	N.º 16, alíneas c), e) e f)
Timothy Kirkhope (ECR)	Âmbito da segurança internacional, europeia e nacional na perspetiva da UE	N.º 16, alíneas a) e b)
AFET 3 membros	Aspetos de política externa do inquérito sobre vigilância eletrónica em larga escala dos cidadãos da UE	N.º 16, alíneas a), b) e f)

ANEXO II: LISTA DE AUDIÇÕES E PERITOS

INQUÉRITO DA COMISSÃO LIBE
SOBRE O PROGRAMA DE VIGILÂNCIA DA NSA DOS EUA,
OS ORGANISMOS DE VIGILÂNCIA EM DIVERSOS ESTADOS-MEMBROS
E O SEU IMPACTO NOS DIREITOS FUNDAMENTAIS DOS CIDADÃOS DA UE E NA COOPERAÇÃO TRANSATLÂNTICA EM MATÉRIA DE JUSTIÇA E ASSUNTOS INTERNOS

Na sequência da Resolução do Parlamento Europeu, de 4 de julho de 2013 (n.º 16), a Comissão LIBE realizou uma séria de audições para recolher informações relacionadas com os diferentes aspetos em causa, avaliar o impacto das atividades de vigilância em questão, nomeadamente nos direitos fundamentais e na regulamentação em matéria de proteção de dados, explorar os mecanismos de recursos e propor recomendações destinadas a proteger os direitos dos cidadãos da UE, assim como a reforçar a segurança informática das Instituições da UE.

Date	Objeto	Especialistas
5 de setembro de 2013 15h00-18h30 (BXL)	– Troca de opiniões com os jornalistas que revelaram o caso e divulgaram os factos ao público	• Jacques FOLLOROU, Le Monde • Jacob APPELBAUM, jornalista de investigação, programador de *software* e investigador de segurança informática com o Tor Project • Alan RUSBRIDGER, chefe de redação da Guardian News and Media (via videoconferência)
	– Acompanhamento da Comissão Temporária sobre o Sistema de Interceção ECHELON	• Carlos COELHO (deputado ao PE), antigo presidente da Comissão Temporária sobre o Sistema de Interceção ECHELON • Gerhard SCHMID (ex-deputado ao PE e relator do relatório sobre o ECHELON, de 2001) • Duncan CAMPBELL, jornalista de investigação e autor do relatório do STOA

		«Interception Capabilities 2000»
12 de setembro de 2013 10h00-12h00 (STR)	– Informações sobre a reunião do grupo de peritos transatlântico UE-EUA sobre a proteção de dados, de 19 e 20 de setembro de 2013 – método de trabalho e cooperação com o Inquérito da Comissão LIBE (à porta fechada) – Troca de pontos de vista com o Grupo do Artigo 29.º para a Proteção de Dados	• Darius ŽILYS, Presidência do Conselho, Diretor do Departamento de Direito Internacional, Ministério da Justiça da Lituânia (copresidente do grupo *ad hoc* UE-EUA sobre a proteção de dados) • Paul NEMITZ, Diretor da DG JUST, Comissão Europeia (copresidente do grupo *ad hoc* UE-EUA sobre a proteção de dados) • Reinhard PRIEBE, Diretor da DG HOME, Comissão Europeia (copresidente do grupo *ad hoc* UE-EUA sobre a proteção de dados) • Jacob KOHNSTAMM, presidente
24 de setembro de 2013 9h00-11h30 e 15h00-18h30 (BXL) **Com a AFET**	– Alegações de interceção, pela NSA, dos dados da SWIFT utilizados no programa TFTP – Informações sobre a reunião do grupo de peritos transatlântico UE-EUA sobre a proteção de dados, de 19 e 20 de setembro de 2013	• Cecilia MALMSTRÖM, membro da Comissão Europeia • Rob WAINWRIGHT, Diretor da Europol • Blanche PETRE, General Counsel da SWIFT • Darius ŽILYS, Presidência do Conselho, Diretor do Departamento de Direito Internacional, Ministério da Justiça da Lituânia (copresidente do grupo *ad hoc* UE-EUA sobre a proteção de dados) • Paul NEMITZ, Diretor da DG JUST, Comissão Europeia (copresidente do grupo *ad hoc* UE-EUA sobre a proteção de dados) • Reinhard PRIEBE, Diretor da DG HOME, Comissão Europeia (copresidente do grupo *ad hoc* UE-EUA sobre a proteção de

		dados)
	– Troca de pontos de vista com a Sociedade Civil dos EUA (parte I)	• Jens-Henrik JEPPESEN, Diretor, Assuntos Europeus, Center for Democracy & Technology (CDT) • Greg NOJEIM, Senior Counsel e Diretor do Project on Freedom, Security & Technology, Center for Democracy & Technology (CDT) (via videoconferência)
	– Eficácia da vigilância na luta contra o crime e o terrorismo na Europa	• Dr Reinhard KREISSL, Coordenador, Increasing Resilience in Surveillance Societies (IRISS) (via videoconferência)
	– Apresentação do estudo sobre os programas de vigilância dos EUA e o seu impacto na privacidade dos cidadãos da UE	• Caspar BOWDEN, investigador independente, antigo Chief Privacy Adviser na Microsoft, autor do documento do Policy Department encomendado pela Comissão LIBE sobre os programas de vigilância dos EUA e o seu impacto na privacidade dos cidadãos da UE
30 de setembro de 2013 15h00-18h30 (BXL) **Com a AFET**	– Troca de pontos de vista com a Sociedade Civil dos EUA (parte II)	• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC) • Catherine CRUMP, American Civil Liberties Union (ACLU)
	– As atividades dos denunciantes no domínio da vigilância e a sua proteção jurídica	Declarações de denunciantes: • Thomas DRAKE, antigo Senior Executive da NSA • J. Kirk WIEBE, antigo analista sénior da NSA • Annie MACHON, antiga agente secreta da MI5 Declarações de ONG sobre a proteção jurídica dos denunciantes: • Jesselyn RADACK, advogada e representante de 6 denunciantes, Government Accountability Project

		• John DEVITT, Transparency International Ireland
3 de outubro de 2013 16h00-18h30 (BXL)	– Alegações de intrusão/interceção dos sistemas Belgacom por serviços de informação (GCHQ do Reino Unido)	• Geert STANDAERT, Vice-Presidente Service Delivery Engine, BELGACOM S.A. • Dirk LYBAERT, Secretário-Geral, BELGACOM S.A. • Frank ROBBEN, Commission de la Protection de la Vie Privée Belgique, correlator do «dossier Belgacom»
7 de outubro de 2013 19h00-21h30 (STR)	– Impacto dos programas de vigilância dos EUA no «porto seguro» – Impacto dos programas de vigilância dos EUA noutros instrumentos de transferências internacionais (cláusulas contratuais, normas empresariais vinculativas)	• Dr. Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (ALEMANHA) • Christopher CONNOLLY – Galexia • Peter HUSTINX, Autoridade Europeia para a Proteção de Dados (AEPD) • **Isabelle FALQUE-PIERROTIN,** Presidente da CNIL (FRANÇA)
14 de outubro de 2013 15h00-18h30 (BXL)	– A vigilância em larga escala eletrónica de cidadãos da UE e internacionais Conselho da Europa e Direito da UE	• Martin SCHEININ, antigo Relator Especial das Nações Unidas sobre a promoção e a defesa dos direitos humanos no âmbito da luta contra o terrorismo, Professor no Instituto Universitário Europeu e líder do projeto FP7 «SURVEILLE» • Judge Bostjan ZUPANČIČ, juiz do TEDH (via videoconferência) • Douwe KORFF, Professor de Direito, London Metropolitan University • Dominique GUIBERT,

	– Processos judiciais sobre programas de vigilância	Vice-Presidente da 'Ligue des Droits de l'Homme' (LDH) • Nick PICKLES, Diretor da Big Brother Watch • Constanze KURZ, cientista de computação, líder de projeto na Forschungszentrum für Kultur und Informatik
7 de novembro de 2013 9h00-11h30 e 15h00-18h30 (BXL)	– O papel do IntCen da UE na atividade de informação da UE (à porta fechada) – Programas nacionais de vigilância em larga escala de dados pessoais nos Estados-Membros da UE e a sua compatibilidade com o direito da UE – O papel do controlo parlamentar dos serviços de informação a nível nacional numa era de vigilância em larga escala (parte I) (Comissão de Veneza) (Reino Unido) – Grupo de peritos transatlântico UE-EUA	• Ilkka SALMI, Diretor do Centro de Análise de Informações da UE (IntCen) • Dr. Sergio CARRERA, Investigador Principal e Chefe da Secção JAI, Centro de Estudos de Política Europeia (CEPS), Bruxelas • Dr. Francesco RAGAZZI, Professor Assistente de Relações Internacionais, Universidade de Leiden • Iain CAMERON, Membro da Comissão Europeia para a Democracia pelo Direito – «Comissão de Veneza» • Ian LEIGH, Professor de Direito, Durham University • David BICKFORD, Antigo Diretor Jurídico das agências de segurança e informação MI5 e MI6 • Gus HOSEIN, Diretor Executivo, Privacy International • Paul NEMITZ, Diretor – Direitos Fundamentais e Cidadania, DG JUST, Comissão Europeia • Reinhard PRIEBE, Diretor – Gestão de Crises e Segurança Interna, DG Home, Comissão Europeia
11 de novembro de 2013 15h00-18h30	– Programas de vigilância dos EUA e os seus impactos na privacidade dos cidadãos da UE (declaração de Jim SENSENBRENNER, Membro	• Jim SENSENBRENNER, Câmara dos Representantes dos EUA (Membro da Comissão Judiciária e Presidente da

(BXL)	do Congresso dos EUA) – O papel do controlo parlamentar dos serviços de informação a nível nacional numa era de vigilância em larga escala (NL, SW) (parte II) – Os programas da NSA dos EUA de vigilância eletrónica em larga escala e papel das empresas de informática (Microsoft, Google, Facebook)	Subcomissão para o Crime, o Terrorismo, a Segurança Nacional e as Investigações) • Peter ERIKSSON, Presidente da Comissão da Constituição, Parlamento sueco (Riksdag) • A.H. VAN DELDEN, Presidente da Comissão Independente de Inquérito Neerlandesa sobre os Serviços de Informação e Segurança (CTIVD • Dorothee BELZ, Vice-Presidente, Legal and Corporate Affairs Microsoft EMEA (Europa, Médio Oriente e África) • Nicklas LUNDBLAD, Director, Public Policy and Government Relations, Google • Richard ALLAN, Director EMEA Public Policy, Facebook
14 de novembro de 2013 15h00-18h30 (BXL) **Com a AFET**	– Segurança informática das Instituições da UE (Parte I) (PE, COM (CERT-UE), (eu-LISA)) – O papel do controlo parlamentar dos serviços de informação a nível nacional numa era de vigilância em larga escala (parte III) (BE, DA)	• Giancarlo VILELLA, Diretor-Geral, DG ITEC, Parlamento Europeu • Ronald PRINS, Diretor e cofundador da Fox-IT • Freddy DEZEURE, chefe da *task force* CERT-UE, DG DIGIT, Comissão Europeia • Luca ZAMPAGLIONE, Responsável pela Segurança, eu-LISA • Armand DE DECKER, Vice-Presidente do Senado belga, Membro da Comissão de Acompanhamento do Comité de Supervisão dos Serviços de Informação • Guy RAPAILLE, Presidente do Comité de Supervisão dos Serviços de Informação (Comité R) • Karsten LAURITZEN, Membro

		da Comissão dos Assuntos Jurídicos, Porta-voz para os Assuntos Jurídicos – Folketing dinamarquês
18 de novembro de 2013 19h00-21h30 (STR)	– Processos judiciais e outras reclamações contra programas de vigilância nacionais (Parte II) ONG polaca)	• Dr Adam BODNAR, Vice-Presidente do Conselho de Administração, Helsinki Foundation for Human Rights (Polónia)
2 de dezembro de 2013 15h00-18h30 (BXL)	– O papel do controlo parlamentar dos serviços de informação a nível nacional numa era de vigilância em larga escala (parte IV) (Noruega)	• Michael TETZSCHNER, membro da Comissão Permanente de Controlo e Assuntos Constitucionais, Noruega (Stortinget)
5 de dezembro de 2013 15h00-18h30 (BXL)	– Segurança informática das Instituições da UE (Parte II) – O impacto da vigilância em larga escala na confidencialidade das relações advogado-cliente	• Olivier BURGERSDIJK, Chefe de Estratégia, Centro Europeu de Cibercriminalidade, EUROPOL • Prof. Udo HELMBRECHT, Diretor Executivo da ENISA • Florian WALTHER, Consultor independente de segurança informática • Jonathan GOLDSMITH, Secretário-Geral, Conselho das Ordens dos Advogados Europeias (CCBE)
9 de dezembro de 2013 (STR)	– Restabelecer a confiança nos fluxos de dados UE-EUA – Resolução 1954 do Conselho da Europa (2013) sobre «Segurança nacional e acesso à informação)	• Viviane REDING, Vice-Presidente da Comissão Europeia • Arcadio DÍAZ TEJERA, Membro do Senado Espanhol, Membro da Assembleia Parlamentar do Conselho da Europa e Relator da sua Resolução 1954 (2013) sobre «Segurança nacional e acesso à informação»
17-18 de dezembro (BXL)	Comissão Parlamentar de Inquérito da espionagem do Senado Brasileiro (Videoconferência)	• Vanessa GRAZZIOTIN, Presidente da Comissão Parlamentar de Inquérito da espionagem • Ricardo DE REZENDE FERRAÇO, Relator da Comissão Parlamentar de Inquérito da espionagem

	Meios informáticos de proteção da privacidade	• Bart PRENEEL, Professor de Segurança Informática e Criptografia Industrial na Universidade KU Leuven, Bélgica • Stephan LECHNER, Diretor, Instituto para a Proteção e Segurança dos Cidadãos (IPSC), – Centro Comum de Investigação (CCI), Comissão Europeia • Dr. Christopher SOGHOIAN, Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union • Christian HORCHERT, Consultor de segurança informática, Alemanha
	Troca de pontos de vista com o jornalista que divulgou os factos (Parte II) (Videoconferência)	• Glenn GREENWALD, autor e colunista dedicado à segurança nacional e às liberdades cívicas, antigo colaborador do *The Guardian*

ANEXO III: LISTA DE PERITOS QUE DECLINARAM O CONVITE PARA PARTICIPAR NAS AUDIÇÕES PÚBLICAS NO ÂMBITO DO INQUÉRITO DA COMISSÃO LIBE

1. Peritos que declinaram o Convite do presidente da Comissão LIBE

EUA

- Keith Alexander, General US Army, Diretor da NSA[1]
- Robert S. Litt, General Counsel, Gabinete do Diretor dos Serviços Nacionais de Informação[2]
- Robert A. Wood, Chargé d'affaires, Representante dos Estados Unidos na União Europeia

Reino Unido

- Sir Iain Lobban, Diretor do Government Communications Headquarters (GCHQ) do Reino Unido

França

- Bernard Bajolet, Directeur général de la Sécurité Extérieure, França
- Patrick Calvar, Directeur Central de la Sécurité Intérieure, França

Países Baixos

- Ronald Plasterk, Ministro do Interior e das Relações do Reino, Países Baixos
- Ivo Opstelten, Ministro da Segurança e da Justiça, Países Baixos

Polónia

- Dariusz Łuczak, Chefe da Agência de Segurança Interna da Polónia
- Maciej Hunia, Chefe da Agência de Informação Externa da Polónia

Empresas de informática privadas

- Tekedra N. Mawakana, Global Head of Public Policy and Deputy General Counsel, Yahoo
- Dr Saskia Horsch, Senior Manager Public Policy, Amazon

[1] O relator reuniu com Keith Alexander, juntamente com o Presidente Elmar Brok e a Senadora Dianne Feinstein em Washington, em 29 de outubro de 2013.
[2] A delegação LIBE reuniu com Robert S. Litt em Washington, em 29 de outubro de 2013.

Empresas de telecomunicações da UE

- Aurelie Doutriaux, Orange
- Larry Stone, President Group Public & Government Affairs British Telecom, Reino Unido
- Telekom, Alemanha
- Vodafone

2. Peritos que não responderam ao convite do presidente da Comissão LIBE

Alemanha

- Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Países Baixos

- Ms. Berndsen-Jansen, Voorzitter Vaste Kamer Commissie voor Binnenlandse Zaken Tweede Kamer der Staten-Generaal, Nederland
- Rob Bertholee, Directeur Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Suécia

- Ingvar Åkesson, Instituto Nacional de Rádio na Área da Defesa (Försvarets radioanstalt, FRA)