Resolução do Parlamento Europeu, de 12 de março de 2014, 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, nomeadamente 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 respetivos protocolos,

– 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 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal do Conselho da Europa (STE 108) e o seu Protocolo Adicional, de 8 de novembro de 2001, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados (STE 181),

– Tendo em conta a Convenção de Viena sobre relações diplomáticas, nomeadamente os seus artigos 24.º, 27.º e 40.º,

– Tendo em conta a Convenção do Conselho da Europa sobre o Cibercrime (STE 185),

– Tendo em conta o relatório do Relator Especial das Nações Unidas sobre a promoção e a proteção dos direitos humanos e das liberdades fundamentais na luta antiterrorista, apresentado em 17 de maio de 2010[2],

– Tendo em conta a Comunicação da Comissão intitulada «A política e a governação da Internet – O papel da Europa na configuração da Internet do futuro» (COM(2014)0072),

– Tendo em conta o relatório do Relator Especial das Nações Unidas sobre a promoção e a proteção do direito à liberdade de opinião e de expressão, apresentado em 17 de abril de 2013[3],

– Tendo em conta as orientações 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, adotada 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[4], 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 instaurados nos tribunais franceses[5], polacos e britânicos[6], assim como no Tribunal Europeu dos Direitos do Homem[7], relativos aos sistemas de vigilância em larga escala,

– Tendo em conta o ato do Conselho que estabelece, em conformidade com o artigo 34.º do Tratado da União Europeia, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia, em particular o seu título III[8],

– 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)0196) e de 20 de outubro de 2004 (SEC(2004)1323),

– Tendo em conta a Comunicação da Comissão, de 27 de novembro de 2013, sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE (**COM(2013)0847**) e a Comunicação da Comissão, de 27 de novembro de 2013, intitulada «Restabelecer a confiança nos fluxos de dados entre a UE e os EUA» (**COM(2013)0846**),

– Tendo em conta a sua resolução, 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[9], que considerou não ser possível confirmar a adequação do sistema, assim como os pareceres do Grupo de Trabalho do Artigo 29.º, em particular o Parecer 4/2000, de 16 de maio de 2000[10],

– Tendo em conta os acordos entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos dados contidos nos registos de identificação dos passageiros (Acordos PNR), de 2004, 2007[11] e 2012[12],

- Tendo em conta relatório da Comissão ao Parlamento Europeu e ao Conselho sobre a revisão conjunta da aplicação do Acordo entre a União Europeia e os Estados Unidos da América sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna (DHS - *Department of Homeland Security*) dos Estados Unidos[13] (**COM(2013)0844**),

– 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, na sua globalidade, incompatível com o artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, sendo o seu artigo 6.º incompatível com o artigo 7.º e o artigo 52.º, n.º 1, da Carta[14],

– 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,[15] 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[16],

– Tendo em conta as negociações em curso relativas ao acordo-quadro UE-EUA sobre a proteção dos dados pessoais transferidos e tratados para efeitos de prevenção, investigação, deteção e repressão de infrações penais, 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 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[17],

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

– Tendo em conta o *USA PATRIOT Act*, 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, promulgado pelo Presidente dos EUA em 1981 e alterado em 2008,

– Tendo em conta a *Presidential Policy Directive (PPD-28) on Signals Intelligence Activities*, promulgada pelo Presidente dos Estados Unidos da América, Barack Obama, em 17 de janeiro de 2014,

– Tendo em conta as propostas legislativas atualmente em exame no Congresso norte-americano, nomeadamente o projeto de *US Freedom Act*, o projeto *Intelligence Oversight* e o *Surveillance Reform Act*,

– Tendo em conta os controlos realizados pelo *Privacy and Civil Liberties Oversight Board* (Conselho de vigilância da vida privada e das liberdades cívicas), pelo Conselho de Segurança Nacional dos EUA e pelo *President's Review Group on Intelligence and Communications Technology* (grupo de peritos do Presidente sobre serviços de informação e tecnologias da comunicação), 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 do *District Court for the District of Columbia* (tribunal de primeira instância para o *District of Columbia*) dos Estados Unidos, Klayman et al. v Obama et al., Processo Civil n.º 13-0851, de 16 de dezembro de 2013, e o acórdão do *District Court for the Southern District of New York* (tribunal de primeira instância para o *Southern District of New York*), ACLU et al. v James R. Clapper et al., de 11 de junho de 2013,

– Tendo em conta o relatório sobre as conclusões dos copresidentes da UE do grupo de trabalho *ad hoc* UE-EUA sobre a proteção dos dados, de 27 de novembro de 2013[18],

– Tendo em conta as suas resoluções, de 5 de setembro de 2001[19] e de 7 de novembro de 2002[20], sobre a existência de um sistema mundial de interceção das 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[21],

– 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 Assuntos Internos de conduzir um inquérito aprofundado sobre a questão[22],

– Tendo em conta o documento de trabalho n.º 1 sobre os programas de vigilância dos EUA e da UE e o seu impacto nos direitos fundamentais dos cidadãos da UE,

– Tendo em conta o documento de trabalho n.º 3 sobre a relação entre as práticas de vigilância na UE e nos EUA e as disposições em matéria de proteção dos dados da UE,

– Tendo em conta o documento de trabalho n.º 4 sobre as atividades de vigilância dos EUA a respeito dos dados da UE e as suas possíveis implicações jurídicas nos acordos e na cooperação transatlânticos,

– Tendo em conta o documento de trabalho n.º 5 sobre o controlo democrático dos serviços de informação dos Estados-Membros e das agências de informação da União Europeia,

– Tendo em conta o documento de trabalho da Comissão AFET sobre os aspetos de política externa do inquérito sobre vigilância eletrónica em larga escala dos cidadãos da UE;

– 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[23],

– 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[24],

– Tendo em conta a sua resolução, de 10 de dezembro de 2013, sobre a exploração plena do potencial da computação em nuvem na Europa[25],

– 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[26],

– 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 (**A7-0139/2014**),

O impacto da vigilância em larga escala

A. Considerando que a proteção dos dados e a vida privada são direitos fundamentais; considerando que, por conseguinte, as medidas de segurança, entre as quais as medidas de luta contra o terrorismo, devem ser aplicadas em conformidade com o Estado de direito e ser subordinadas às obrigações em matéria de direitos fundamentais, nomeadamente no que se refere à vida privada e à proteção dos dados;

B. Considerando que os dados e os fluxos de informação, que dominam a vida quotidiana atual e constituem parte da integridade de qualquer pessoa, têm de estar tão protegidos contra a intrusão

como os domicílios privados;

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

D. Considerando que a cooperação entre os Estados Unidos e a UE e os seus Estados-Membros no âmbito da luta contra o terrorismo continua a revestir uma importância vital para a segurança de ambos os parceiros;

E. Considerando que a confiança e o entendimento mútuos são fatores fundamentais no diálogo e na parceria transatlânticos;

F. Considerando que, no seguimento dos acontecimentos de 11 de setembro de 2001, a luta contra o terrorismo passou a ser uma das principais prioridades da maioria dos governos; considerando que as revelações baseadas nos documentos divulgados por Edward Snowden, antigo colaborador da NSA, obrigam os líderes políticos a responder aos desafios em matéria de supervisão e controlo das atividades de vigilância das agências de informação e de avaliação do impacto das suas atividades nos direitos fundamentais e no Estado de direito nas sociedades democráticas;

G. Considerando que as revelações feitas desde junho de 2013 têm causado preocupação na UE no que diz respeito:

– à envergadura dos sistemas de vigilância revelados tanto nos Estados Unidos como nos Estados-Membros da UE;
– à violação das normas do direito da UE, dos direitos fundamentais e das normas relativas à proteção dos dados;
– ao grau de confiança entre a UE e os Estados Unidos enquanto parceiros transatlânticos;
– ao grau de cooperação e participação de alguns Estados-Membros da UE nos programas de vigilância dos EUA ou em programas equivalentes a nível nacional revelados pelos meios de comunicação social;
– à falta de controlo e de supervisão eficazes por parte das autoridades políticas norte-americanas e de certos Estados-Membros da UE sobre os seus serviços de informação;
– à possibilidade de estas operações de vigilância em larga escala serem utilizadas por motivos não estritamente ligados à segurança nacional e à luta contra o terrorismo, nomeadamente para fins de espionagem económica e industrial ou de definição de perfis por razões políticas;
– à limitação da liberdade de imprensa e das comunicações dos profissionais que detêm um privilégio de confidencialidade, como é do caso dos advogados e dos médicos;
– aos 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 e submetidos a vigilância;
– às ameaças à vida privada na era digital e ao impacto da vigilância em larga escala nos cidadãos e nas sociedades;

H. Considerando que a revelação de uma espionagem de envergadura sem precedentes requer um inquérito cabal por parte das autoridades norte-americanas, das instituições europeias e dos governos, parlamentos nacionais e autoridades judiciais dos Estados-Membros;

I. Considerando que as autoridades norte-americanas negaram algumas das informações reveladas, mas não contestaram a grande maioria das informações; considerando que o debate público assumiu grandes proporções nos Estados Unidos e em alguns Estados-Membros da UE; considerando que os governos e os parlamentos da UE se mantêm demasiadas vezes em silêncio, abstendo-se de lançar inquéritos adequados;

J. Considerando que o Presidente Obama anunciou recentemente a reforma da NSA e dos seus programas de vigilância;

K. Considerando que, à semelhança das ações tomadas tanto pelas instituições da UE como por alguns dos seus Estados-Membros, o Parlamento Europeu assumiu com seriedade a sua obrigação de clarificar as revelações relativas às práticas indiscriminadas de vigilância em larga escala dos cidadãos da UE e, através da 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, encarregou a sua Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos de conduzir um inquérito aprofundado sobre a questão;

L. Considerando que incumbe às Instituições europeias velar por que o direito da UE seja plenamente aplicado no interesse dos cidadãos europeus e por que a força jurídica dos Tratados da UE não seja comprometida por uma banal aceitação dos efeitos extraterritoriais das normas ou ações de países terceiros;

Evolução da reforma dos serviços de informação nos Estados Unidos

M. Considerando que o *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[(27)]; considerando, no entanto, que o *District Court for the Southern District of New York* determinou, por decisão de 27 de dezembro de 2013, que esta recolha é legal;

N. Considerando que uma decisão do *District Court for the Eastern District of Michigan* (tribunal de primeira instância para o *Eastern District of Michigan*) determinou que a Quarta Emenda requer a realização de pesquisas razoáveis, mandados prévios para todas as buscas razoáveis, mandados baseados numa causa provável pré-existente, assim como a tomada em consideração da particularidade das pessoas, dos locais e das coisas e a interposição de um magistrado neutro entre os agentes repressivos do poder executivo e os cidadãos[(28)];

O. Considerando que, no seu relatório de 12 de dezembro de 2013, o Grupo de Peritos do Presidente sobre Serviços de Informação e Tecnologias da Comunicação propõe 46 recomendações ao Presidente dos EUA; considerando que essas recomendações salientam a necessidade de proteger simultaneamente a segurança nacional e a vida privada das pessoas e as liberdades cívicas; considerando que, neste contexto, convida o Governo dos Estados Unidos a tomar as seguintes medidas: pôr termo, o mais rapidamente possível, à recolha em larga escala de registos telefónicos de cidadãos norte-americanos ao abrigo da secção 215 do *Patriot Act*; proceder a uma revisão profunda do quadro jurídico da NSA e dos serviços de informação norte-americanos para assegurar o respeito pelo direito à vida privada; pôr termo aos esforços no sentido de corromper ou tornar vulnerável o software comercial (falhas de segurança e software malicioso); intensificar a utilização de técnicas de encriptação, em particular no caso de dados em trânsito, e não comprometer os esforços de criação de normas de encriptação; designar um representante do interesse público para defender a vida privada e as liberdades cívicas no *Foreign Intelligence Surveillance Court* (tribunal de vigilância dos serviços de informação externos); conferir à Comissão de Controlo da Vida Privada e das Liberdades Cívicas o poder de supervisionar as atividades dos serviços de informação no que diz respeito à informação externa e não apenas para fins de luta contra o terrorismo; receber queixas de denunciantes, utilizar os tratados de auxílio judiciário mútuo para obter comunicações eletrónicas e não recorrer à vigilância para roubar segredos industriais ou comerciais;

P. Considerando que, de acordo com um memorando aberto apresentado ao Presidente Obama pelos *Former NSA Senior Executives/Veteran Intelligence Professionals for Sanity - VIPS* (antigos altos responsáveis da NSA), em 7 de janeiro de 2014[(29)], a recolha de dados em grande escala não reforça a capacidade da NSA para prevenir futuros ataques terroristas; considerando que os autores salientam que a vigilância em grande escala efetuada pela NSA não preveniu qualquer ataque e que se gastaram milhares de milhões de dólares em programas que são menos eficazes e muito mais

invasivos da vida privada dos cidadãos do que a tecnologia interna denominada THINTHREAD, criada em 2001;

Q. Considerando que, no que respeita às atividades de informação sobre cidadãos não norte-americanos ao abrigo da secção 702 do FISA, as recomendações ao Presidente dos EUA reconhecem o princípio fundamental do respeito pela vida privada 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 essas recomendações não preconizam a concessão aos cidadãos não nacionais dos Estados Unidos dos mesmos direitos e proteções concedidos aos cidadãos norte-americanos;

R. Considerando que, na *Presidential Policy Directive on Signals Intelligence Activities*, de 17 de janeiro de 2014, o Presidente dos Estados Unidos, Barack Obama, salientou que a vigilância eletrónica em grande escala era necessária para assegurar a segurança nacional, proteger os cidadãos norte-americanos e os cidadãos dos países aliados e parceiros dos Estados Unidos, bem como promover os interesses da política externa; considerando que esta diretiva estratégica contém princípios em matéria de recolha, utilização e partilha de informações sobre transmissões e estende determinadas garantias aos cidadãos não nacionais dos Estados Unidos, prevendo um tratamento parcialmente equivalente ao concedido aos cidadãos norte-americanos, nomeadamente garantias relativas aos dados pessoais de todos os indivíduos, independentemente da sua nacionalidade ou residência; considerando, todavia, que o Presidente Obama não apelou à apresentação de propostas concretas, em particular no que se refere à proibição das atividades de vigilância em larga escala e à interposição de recursos judiciais e administrativos por cidadãos estrangeiros;

Quadro jurídico Direitos fundamentais

S. Considerando que o relatório sobre as conclusões dos copresidentes da União do grupo de trabalho *ad hoc* UE-EUA sobre a proteção dos dados fornece uma visão global da situação jurídica nos EUA, mas não apura factos no que se refere aos programas de vigilância dos EUA; considerando que não foi disponibilizada qualquer informação sobre o grupo de trabalho dito de «segunda via», no âmbito da qual os Estados-Membros debatem bilateralmente com as autoridades norte-americanas questões relacionadas com a segurança nacional;

T. 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 e à proteção dos dados, bem como o direito de recurso, a presunção de inocência e o direito a um processo equitativo 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; considerando que a vigilância em larga escala de seres humanos é incompatível com estes princípios;

U. Considerando que em todos o Estados-Membros a lei protege os cidadãos contra a divulgação de informação comunicada a título confidencial entre um advogado e o seu cliente, princípio que foi reconhecido pelo Tribunal da Justiça da União Europeia[(30)];

V. Considerando que, na sua resolução de 23 de outubro de 2013, sobre a criminalidade organizada, a corrupção e o branqueamento de capitais, o Parlamento solicita à Comissão que apresente uma proposta legislativa que estabeleça um programa europeu eficaz e abrangente para a proteção dos autores de denúncias, a fim de proteger os interesses financeiros da UE, e que, além disso, efetue um estudo sobre a oportunidade de essa futura legislação ser estendida a outros domínios de competência da União;

Competências da União no domínio da segurança

W. 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 e os artigos 72.º e 73.º do TFUE) implicam que a UE disponha de

determinadas competências em questões relacionadas com a segurança coletiva da União; considerando que a UE tem competência em matéria de segurança interna (artigo 4.º, alínea j), do TFUE) e que exerceu esta competência adotando uma série de instrumentos legislativos e celebrando acordos internacionais (PNR, TFTP) destinados a combater formas graves de criminalidade e o terrorismo, bem como criando uma estratégia de segurança interna e agências que operam neste domínio;

X. Considerando que o Tratado sobre o Funcionamento da União Europeia estabelece que «os Estados-Membros são livres de organizar entre si e sob a sua responsabilidade formas de cooperação e de coordenação, conforme considerarem adequado, entre os serviços competentes das respetivas administrações responsáveis pela garantia da segurança nacional» (artigo 73.º do TFUE);

Y. Considerando que o artigo 276.º do TFUE estabelece que «no exercício das suas atribuições relativamente às disposições dos Capítulos 4 e 5 do Título V da Parte III, relativas ao espaço de liberdade, segurança e justiça, o Tribunal de Justiça da União Europeia não é competente para fiscalizar a validade ou a proporcionalidade de operações efetuadas pelos serviços de polícia ou outros serviços responsáveis pela aplicação da lei num Estado-Membro, nem para decidir sobre o exercício das responsabilidades que incumbem aos Estados-Membros em matéria de manutenção da ordem pública e de garantia da segurança interna»;

Z. 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 interferir nas competências da UE;

AA. Considerando que os Tratados europeus conferem à Comissão Europeia o papel de «guardiã dos Tratados», pelo que esta Instituição é legalmente responsável pela investigação de todas as potenciais violações do direito da União;

AB. Considerando que, nos termos do artigo 6.º do TUE, que se refere à Carta dos Direitos Fundamentais da União Europeia e à Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH), as agências dos Estados-Membros e as entidades privadas que operam no domínio da segurança nacional devem respeitar os direitos consagrados nesses atos, tanto no que se refere aos seus cidadãos como aos cidadãos de outros Estados;

Extraterritorialidade

AC. 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 ter repercussões no ordenamento jurídico estabelecido e no Estado de direito, ou mesmo violar o direito internacional ou da União, nomeadamente os direitos das pessoas singulares e coletivas, consoante o grau e o objetivo declarado ou efetivo de tal aplicação; considerando que, nestas circunstâncias, é necessário tomar medidas a nível da União para garantir o respeito no seu território dos valores da UE consagrados no artigo 2.º do TUE, na Carta dos Direitos Fundamentais, na CEDH, no que se refere aos direitos fundamentais, à democracia e ao Estado de direito, bem como os direitos das pessoas singulares e coletivas consagrados nos atos de direito derivado que aplicam estes princípios fundamentais, nomeadamente através da eliminação, neutralização, bloqueio ou de qualquer outra forma de oposição aos efeitos da legislação estrangeira em causa;

Transferências internacionais de dados

AD. Considerando que a transferência de dados pessoais pelas instituições, órgãos, serviços ou agências da UE ou pelos Estados-Membros para os Estados Unidos 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 vida privada e à proteção dos 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[(31)], por uma violação do direito da União – que inclui qualquer violação dos direitos fundamentais consagrados na Carta dos Direitos Fundamentais da UE;

AE. Considerando que a transferência de dados não é geograficamente limitada, e que, em particular no contexto da crescente globalização e das comunicações à escala mundial, o legislador da UE é confrontado com novos desafios em matéria de proteção dos dados pessoais e das comunicações; considerando que é, por conseguinte, extremamente importante promover quadros jurídicos com normas comuns;

AF. Considerando que a recolha de dados pessoais em grande escala para efeitos comerciais e no âmbito da luta contra o terrorismo e as formas graves de criminalidade transnacional põem em risco os dados pessoais e o direito à vida privada dos cidadãos da UE;

Transferências para os Estados Unidos baseadas no princípio do «porto seguro»

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

AH. Considerando que, a fim de permitir que os responsáveis pelo tratamento de dados da UE transfiram dados pessoais para uma entidade norte-americana, a Comissão, na sua Decisão 200/520/CE, considerou adequado o nível de proteção assegurado pelos «princípios da viva privada em porto seguro» e pelas FAQ que lhes dizem respeito, publicadas pelo Departamento do Comércio dos Estados Unidos, para os dados pessoais transferidos da União para organizações estabelecidas nos EUA que tenham aderido aos princípios de «porto seguro»;

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

AJ. Considerando que, no seu documento de trabalho n.º 4 sobre as atividades de vigilância dos Estados Unidos no que diz respeito aos dados da UE e às suas possíveis implicações jurídicas nos acordos e na cooperação transatlânticos, de 12 de dezembro de 2013, os relatores expressaram dúvidas e preocupação em relação à adequação do «porto seguro» e instaram a Comissão a revogar a decisão relativa à adequação do «porto seguro» e a encontrar novas soluções jurídicas;

AK. Considerando que a Decisão 2000/520/CE da Comissão estabelece 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 razões para crer 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;

AL. Considerando que a Decisão 2000/520/CE da Comissão estabelece igualmente que, se dispuser de elementos que demonstrem que os organismos responsáveis pelo cumprimento dos princípios não desempenham eficazmente as suas funções, a Comissão deve informar o Departamento de Comércio norte-americano e, se necessário, apresentar um projeto de medidas para revogar ou suspender a decisão ou limitar o seu âmbito;

AM. Considerando que, nos seus dois primeiros relatórios sobre a aplicação do «porto seguro», publicados em 2002 e 2004, a Comissão identificou várias deficiências relativamente à aplicação adequada do «porto seguro» e formulou diversas recomendações às autoridades dos EUA tendo em vista a correção dessas deficiências;

AN. Considerando que, no seu terceiro relatório de execução, de 27 de novembro de 2013, nove anos após o segundo relatório e sem que as deficiências apontadas neste último tivessem sido corrigidas, a Comissão identificou outras deficiências e lacunas generalizadas no «porto seguro» e concluiu que a aplicação, nos termos atualmente em vigor, não podia manter-se; considerando que a Comissão salientou que o acesso generalizado das agências de informação norte-americanas aos dados transferidos para os Estados Unidos por entidades que aderiram ao «porto seguro» coloca questões graves adicionais relativas à continuidade da proteção dos dados de titulares cidadãos da UE; considerando que a Comissão dirigiu 13 recomendações às autoridades norte-americanas e se comprometeu a identificar, até ao verão de 2014, juntamente com essas autoridades, soluções a aplicar logo que possível, que constituirão a base de uma revisão completa do funcionamento dos princípios de «porto seguro»;

AO. Considerando que, em 28-31 de outubro de 2013, uma delegação da Comissão das Liberdades Civis, da Justiça e dos Assuntos Internos (Comissão LIBE) do Parlamento Europeu se reuniu em Washington D.C. com o Departamento do Comércio e com Comissão Federal do Comércio dos Estados Unidos; considerando que o Departamento do Comércio reconheceu a existência de organizações que apresentaram a sua declaração de adesão aos princípios de «porto seguro», mas que têm claramente um estatuto de certificação «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 do Comércio admitiu que o «porto seguro» deveria ser revisto e melhorado, em particular no que diz respeito aos sistemas de reclamações e de resolução alternativa de litígios;

AP. Considerando que os princípios de «porto seguro» podem ser limitados à medida necessária para observar requisitos de segurança nacional, interesse público ou de aplicação da lei; considerando que uma exceção a um direito fundamental deve ser sempre interpretada de forma restritiva e limitada ao que é necessário e proporcional numa sociedade democrática, devendo a lei definir claramente as condições e garantias que tornam essa limitação legítima; considerando que o âmbito de aplicação de tal exceção deveria ter sido clarificado pelos Estados Unidos e pela UE, nomeadamente pela Comissão, a fim de evitar toda a interpretação ou aplicação que anule na substância o direito fundamental à vida privada e à proteção de dados, entre outros; considerando, por conseguinte, que uma tal exceção não deve ser utilizada de forma a comprometer ou anular a proteção concedida pela Carta dos Direitos Fundamentais, pela CEDH, pela legislação da União em matéria de proteção de dados e pelos princípios de «porto seguro»; insiste em que, caso seja invocada a exceção da segurança nacional, seja especificada a legislação nacional em que a mesma se apoia;

AQ. Considerando que o acesso em larga escala à informação pelas agências de informação norte-americanas corroeu seriamente a confiança transatlântica e teve um impacto negativo na confiança nas organizações dos Estados Unidos que operam na UE; considerando que esta situação é agravada pela falta de acesso a recurso judicial e administrativo para os cidadãos da UE, na legislação norte-americana, em particular nos casos de atividades de vigilância para efeitos de informação;

Transferências para países terceiros acompanhadas de decisão de adequação

AR. 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, do Canadá e da Austrália estiveram associadas à vigilância em larga escala de comunicações eletrónicas e cooperaram ativamente com os Estados Unidos no chamado programa *Five Eyes*, podendo ter trocado entre si dados pessoais de cidadãos da UE transferidos da UE;

AS. Considerando que as Decisões 2013/65/UE[(32)] e 2002/2/CE[(33)], da Comissão declararam adequado o nível de proteção assegurado pelo *Privacy Act* da Nova Zelândia e pelo *Personal Information Protection and Electronic Documents Act* do Canadá; considerando que as revelações supramencionadas afetam também 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

AT. 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 forneça garantias adequadas no que se refere à proteção dos direitos e liberdades fundamentais e da vida privada dos indivíduos e ao exercício dos direitos correspondentes;

AU. Considerando que estas garantias podem, em particular, resultar de cláusulas contratuais adequadas;

AV. Considerando que a Diretiva 95/46/CE confere poderes à Comissão para decidir que determinadas 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-tipo para transferências para os responsáveis pelo tratamento e subcontratantes (e subcontratantes ulteriores) em países terceiros;

AW. 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 se determine que a legislação a que o importador de dados ou um subcontratante 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;

AX. Considerando que as autoridades nacionais de proteção de dados elaboraram normas vinculativas para as empresas destinadas a facilitar as transferências internacionais numa 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 vinculativas para as empresas devem ser autorizadas pelas autoridades competentes dos Estados-Membros depois de estas terem avaliado a conformidade com a legislação da União em matéria de proteção de dados; considerando que as normas vinculativas para as empresas destinadas aos subcontratantes foram rejeitadas no relatório da Comissão LIBE sobre o regulamento geral relativo à proteção de dados, pelo facto de retirarem ao responsável pelo tratamento dos dados e ao titular dos dados qualquer possibilidade de controlo sobre a jurisdição em que os seus dados são tratados;

AY. Considerando que o Parlamento Europeu, dadas as competências que lhe atribui o artigo 218.º do TFUE, é responsável pelo controlo permanente do valor dos acordos internacionais que aprovou;

Transferências baseadas nos acordos TFTP e PNR

AZ. Considerando que, na sua resolução de 23 de outubro de 2013, o Parlamento Europeu manifestou sérias preocupações com as revelações relativas às atividades da NSA no que se refere ao acesso direto a mensagens de pagamentos financeiros e dados conexos, que constituiriam uma clara violação do Acordo TFTP, nomeadamente do seu artigo 1.º;

BA. Considerando que a deteção do financiamento do terrorismo é uma ferramenta essencial para lutar contra o financiamento do terrorismo e as formas graves de criminalidade, permitindo que os investigadores nesta matéria descubram ligações entre as pessoas objeto de investigação e outros potenciais suspeitos associados a amplas redes terroristas suspeitas de financiar o terrorismo;

BB. Considerando que o Parlamento 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; considerando que a Comissão não acedeu a nenhum dos pedidos;

BC. Considerando que, na sequência das alegações publicadas pelos meios de comunicação social, a Comissão decidiu iniciar consultas com os Estados Unidos nos termos do artigo 19.º do Acordo TFTP; considerando que, em 27 de novembro de 2013, a Comissária Cecilia Malmström comunicou à Comissão LIBE 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 norte-americano tivesse agido de forma contrária ao disposto no acordo e que os Estados Unidos forneceram uma garantia por escrito de que não fora efetuada qualquer recolha de dados direta contrária às disposições do acordo TFTP; considerando que não foi claramente apurado que as autoridades norte-americanas contornaram o Acordo ao aceder a estes dados por outros meios, como indicado na carta, de 18 de setembro de 2013, das referidas autoridades[(34)];

BD. Considerando que, durante uma visita a Washington, de 28 a 31 de outubro de 2013, a delegação da Comissão LIBE reuniu com o Departamento do Tesouro norte-americano; considerando que o Departamento do Tesouro declarou que, desde a entrada em vigor do Acordo TFTP, apenas teve acesso a dados SWIFT da UE no âmbito do TFTP; considerando que o Departamento do Tesouro se recusou a comentar a eventualidade de o acesso aos dados do SWIFT ter sido efetuado à margem do TFTP por outro órgão ou departamento governamental dos Estados Unidos ou de a administração deste país ter tido conhecimento das atividades de vigilância em larga escala da NSA; considerando que, em 18 de dezembro de 2013, Glenn Greenwald declarou, no âmbito do inquérito realizado pela Comissão LIBE, que a NSA e o GCHQ tinham visado as redes SWIFT;

BE. Considerando que as autoridades de proteção de dados belgas e neerlandesas decidiram, em 13 de novembro de 2013, realizar um inquérito conjunto sobre a segurança das redes de pagamento SWIFT a fim de apurar se terceiros poderiam obter um acesso não autorizado ou ilegal aos dados bancários dos cidadãos europeus[(35)];

BF. Considerando que, de acordo com a revisão conjunta UE-EUA do Acordo PNR, o Departamento da Segurança Interna norte-americano efetuou 23 divulgações de dados PNR à NSA, numa base casuística, no quadro de casos de luta contra o terrorismo, e no pleno respeito das condições específicas do Acordo;

BG. Considerando que a revisão conjunta não refere o facto de que, no caso do tratamento de dados pessoais para efeitos de informação, ao abrigo da legislação norte-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 dos Estados Unidos; 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

BH. Considerando que o Acordo UE-EUA sobre auxílio judiciário mútuo em matéria penal, de 6 de junho de 2003[(36)], entrou em vigor em 1 de fevereiro de 2010 e se destina a facilitar a cooperação entre a UE e os Estados Unidos 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»)

BI. Considerando que o objetivo deste acordo global é estabelecer o quadro jurídico para todas as transferências de dados pessoais entre a UE e os Estados Unidos 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; considerando que este acordo é extremamente importante e

serviria de base para facilitar a transferência de dados no contexto da cooperação policial e judicial e em matéria penal;

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

BK. Considerando que, na sua Comunicação, de 27 de novembro de 2013, a Comissão indicou que o «acordo global» deveria implicar um elevado nível de proteção dos cidadãos de ambos os lados do Atlântico e deveria reforçar a confiança dos europeus nas trocas de dados UE-EUA, criando uma base para o desenvolvimento da cooperação e da parceria UE-EUA em matéria de segurança;

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

Reforma no domínio da proteção dos dados

BM. Considerando que o quadro jurídico da UE em matéria de proteção dos dados está atualmente a ser revisto a fim de criar um sistema abrangente, coerente, moderno e sólido 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 relativo à proteção de dados[(37)], que irá substituir a Diretiva 95/46/CE e estabelecer uma legislação uniforme na UE, e uma diretiva[(38)] que criará um quadro harmonizado para todas as atividades de tratamento de dados realizadas pelas autoridades responsáveis pela aplicação da lei para efeitos de aplicação da lei e reduzirá as divergências existentes entre as legislações nacionais;

BN. 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;

BO. Considerando que, apesar de o Conselho Europeu de 24-25 de outubro de 2013 ter apelado à adoção atempada de um sólido quadro geral da UE para a proteção dos dados, a fim de promover a confiança dos cidadãos e das empresas na economia digital, o Conselho, após dois anos de deliberações, foi incapaz de definir a uma abordagem global sobre o regulamento geral relativo à proteção de dados e sobre a diretiva[(39)];

Segurança informática e computação em nuvem

BP. Considerando que, na sua resolução de 10 de dezembro de 2013, o Parlamento salienta o potencial económico da computação em nuvem para o crescimento e o emprego; considerando que o valor económico global do mercado em nuvem deverá atingir 207 mil milhões de dólares por ano até 2016, ou seja, o dobro do seu valor em 2012;

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

BR. Considerando que as atividades de vigilância em larga escala permitem às agências de informação ter acesso a dados pessoais armazenados ou submetidos a outro tratamento pelos cidadãos da UE ao abrigo de acordos de serviços de computação em nuvem com os principais

prestadores de serviços de computação em nuvem dos Estados Unidos; considerando que os serviços de informação norte-americanos tiveram acesso a dados pessoais armazenados ou tratados em servidores localizados no território da UE intercetando as redes internas Yahoo e Google; considerando que estas atividades constituem uma violação das obrigações internacionais e das normas europeias em matéria de direitos fundamentais, nomeadamente, o direito à vida privada e familiar, à confidencialidade das comunicações, à presunção de inocência, à liberdade de expressão, à liberdade de informação, à liberdade de reunião e de associação e à liberdade de empresa; considerando que não é impossível que os serviços de informação tenham também tido acesso a informações armazenadas em serviços de computação em nuvem pelas autoridades públicas ou empresas e instituições dos Estados-Membros;

BS. Considerando que as agências de informação dos Estados Unidos têm uma política que consiste em corromper sistematicamente os protocolos e produtos criptográficos para poderem intercetar mesmo as comunicações criptadas; considerando que a Agência Nacional de Segurança norte-americana recolheu um grande número de «vulnerabilidades dia zero», ou seja, vulnerabilidades da segurança informática de que o público e o fornecedor do produto ainda não têm conhecimento; que estas atividades prejudicam consideravelmente os esforços mundiais no sentido de melhorar a segurança informática;

BT. Considerando que o facto de as agências de informação terem tido acesso a dados pessoais de utilizadores dos serviços em linha alterou seriamente a confiança dos cidadãos nesses serviços, tendo, por isso, um efeito negativo nas empresas que investem no desenvolvimento de novos serviços que utilizam grandes volumes de dados e novas aplicações, tais como a «Internet das Coisas»;

BU. Considerando que os fornecedores de tecnologias da informação disponibilizam frequentemente produtos cuja segurança informática não foi adequadamente testada ou que têm, por vezes, falhas de segurança que são integradas intencionalmente pelo fornecedor; considerando que a ausência de normas em matéria de responsabilidade dos fornecedores de software tem conduzido a esta situação, que é, por sua vez, explorada pelas agências de informação, mas que abre também a via aos ataques por parte de outras entidades;

BV. Considerando que é essencial que as empresas que prestam estes novos serviços e aplicações respeitem as normas relativas à proteção dos dados e à vida privada dos titulares cujos dados são recolhidos, tratados e analisados com vista a manter a confiança dos cidadãos a um nível elevado;

Controlo democrático dos serviços de informação

BW. Considerando que, nas sociedades democráticas, os serviços de informação dispõem de poderes e meios para proteger os direitos fundamentais, a democracia e o Estado de direito, os direitos dos cidadãos e o Estado contra graves ameaças internas e externas e são objeto de controlo democrático e judicial; considerando que são conferidas a estes serviços competências e capacidades especiais unicamente para este efeito; considerando que estes poderes devem ser utilizados no respeito dos limites jurídicos impostos pelos direitos fundamentais, pela democracia e pelo Estado de direito e que a sua utilização deve ser rigorosamente controlada, pois, caso contrário, perdem legitimidade e podem prejudicar a democracia;

BX. Considerando que, se for concedido um certo nível de sigilo aos serviços de informação para evitar que as operações em curso sejam comprometidas, que o *modus operandi* seja divulgado ou que os agentes possam correr risco de vida, tal sigilo não pode sobrepor-se ou excluir as normas em matéria de controlo e exame democráticos e judiciais das suas atividades, bem como em matéria de transparência, nomeadamente no que se refere ao respeito pelos direitos fundamentais, pela democracia e pelo Estado de direito;

BY. Considerando que a maior parte dos mecanismos e órgãos de controlo nacionais existentes foram criados ou reorganizados na década de 1990 e não foram necessariamente adaptados aos rápidos progressos tecnológicos e à evolução política da última década, que levaram os serviços de informação a uma maior cooperação à escala internacional, nomeadamente através do intercâmbio

de dados pessoais, criando frequentemente uma fronteira pouco nítida entre as atividades de informação e de aplicação da lei;

BZ. Considerando que o controlo democrático das atividades de informação ainda é efetuado apenas 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 dá origem a um controlo democrático insuficiente e ineficaz;

CA. Considerando que, muitas vezes, os órgãos nacionais de controlo não têm pleno acesso às informações fornecidas por uma agência de informação externa, o que pode criar zonas em que os intercâmbios internacionais de informações podem ocorrer sem um controlo adequado; considerando que este problema é agravado pela chamada «regra dos terceiros» ou pelo princípio do «controlo pela entidade de origem», que foi concebido para permitir que a entidade de origem mantenha o controlo sobre a difusão ulterior das suas informações sensíveis, mas que é frequentemente interpretado como sendo também aplicável ao controlo dos serviços da entidade destinatária;

CB. Considerando que as iniciativas de reforma da transparência dos setores público e privado são essenciais para assegurar a confiança do público nas atividades das agências de informação; considerando que os sistemas jurídicos não devem impedir as empresas de divulgar ao público a forma como tratam todos os tipos de pedidos do governo e decisões judiciais para o acesso aos dados dos seus utilizadores, incluindo a possibilidade de divulgar informação agregada sobre o número de pedidos e decisões aprovadas e rejeitadas;

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, o reconhecimento por parte das autoridades e a resposta insuficiente a estas alegações resultaram em provas consistentes da existência de sistemas de longo alcance, complexos e altamente avançados em termos tecnológicos, concebidos pelos serviços de informação dos Estados Unidos e de alguns Estados-Membros, para recolher, armazenar e analisar dados de comunicação, incluindo conteúdos de dados, dados de localização e metadados de todos os cidadãos do mundo a uma escala sem precedentes e de forma indiscriminada e sem base em suspeitas;

2. Salienta especificamente os programas de informação da NSA dos Estados Unidos, 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), o programa de descodificação (Edgehill), os ataques «intrusos» direcionados aos sistemas de informação (programas Quantumtheory e Foxacid) e a recolha e a conservação de 200 milhões de mensagens de texto por dia (programa Dishfire);

3. Constata as alegações de intrusão ou interceção dos sistemas Belgacom pela agência de informação do Reino Unido GCHQ; toma nota das declarações da Belgacom de que não pôde confirmar nem negar se as instituições da UE foram atacadas ou afetadas, e de que o malware utilizado era extremamente complexo e o seu desenvolvimento e utilização exigia importantes recursos financeiros e humanos, o que indica que não estará disponível para entidades ou «hackers» privados;

4. Salienta que a confiança foi profundamente abalada: a confiança entre os dois parceiros transatlânticos, a confiança entre os cidadãos e os seus governos, a confiança no funcionamento das instituições democráticas em ambos os lados do Atlântico, a confiança no respeito pelo Estado de direito e a confiança na segurança dos serviços e comunicações informáticos; acredita que, para restabelecer a confiança em todas estas dimensões, é urgentemente necessário um plano de resposta abrangente que inclua uma série de medidas sujeitas a controlo público;

5. Observa que vários governos alegam que estes programas de vigilância em larga escala são necessários para combater o terrorismo; denuncia veementemente o terrorismo, mas defende firmemente que a luta contra o terrorismo nunca pode constituir uma justificação para programas de vigilância indiscriminada em larga escala, secretos ou mesmo ilegais; considera que tais programas são incompatíveis com os princípios da necessidade e da proporcionalidade numa sociedade democrática;

6. Recorda a firme convicção da UE na necessidade de lograr o justo equilíbrio entre medidas de segurança e proteção das liberdades cívicas e dos direitos fundamentais, assegurando, ao mesmo tempo, o máximo respeito pela privacidade e pela proteção de dados;

7. Considera que uma recolha de dados de tal magnitude deixa dúvidas sobre se estas ações são apenas motivadas pela luta contra o terrorismo, uma vez que envolvem a recolha de todos os dados possíveis de todos os cidadãos; aponta, por conseguinte, para a possível existência de outras motivações, incluindo a espionagem política e económica, as quais devem ser dissipadas na totalidade;

8. 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»;

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

10. Condena a recolha vasta, sistémica e generalizada de dados pessoais de cidadãos inocentes, incluindo frequentemente informações pessoais do foro íntimo; salienta 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 e na liberdade de reunião e de associação, implicando, além disso, um potencial significativo de utilização abusiva das informações recolhidas contra adversários políticos; enfatiza que estas atividades de vigilância em larga escala comportam também ações ilegais por parte dos serviços de informação e suscitam questões relativas à extraterritorialidade das legislações nacionais;

11. Considera ser essencial que o privilégio de confidencialidade profissional de que beneficiam os advogados, jornalistas, médicos e outras profissões regulamentadas constituía uma salvaguarda contra atividades de vigilância em larga escala; salienta, em particular, que qualquer incerteza quanto à confidencialidade das comunicações entre advogados e respetivos clientes poderá ter um impacto negativo no direito que assiste aos cidadãos da UE de acesso a aconselhamento e de acesso à justiça e a um julgamento imparcial;

12. 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 em que qualquer interferência nos direitos fundamentais dos suspeitos deve ser autorizada por um juiz ou procurador com base numa suspeita razoável e deve ser regulamentada pela lei, e promovendo, em vez disso, um misto de atividades de aplicação da lei e de informação com garantias jurídicas pouco nítidas e enfraquecidas, 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[(40)] sobre a proibição da utilização de rastreios sistemáticos de caráter preventivo («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;

13. Está convencido de que legislação 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, a transferência de dados pessoais, não pode ser reconhecido ou aplicado de nenhum modo, a menos que exista um Tratado de Auxílio Judiciário Mútuo ou um acordo internacional em vigor entre o país terceiro requerente e a União ou um Estado-Membro e uma autorização prévia da autoridade de supervisão competente; recorda que qualquer acórdão de um tribunal secreto e qualquer decisão de uma autoridade administrativa de um Estado não pertencente à UE que autorize secretamente, direta ou indiretamente, atividades de vigilância não será reconhecido ou aplicado;

14. Destaca que as preocupações supramencionadas são agravadas pela rápida evolução tecnológica e societal, 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 alicerça num tratamento de dados pessoais; considera que a dimensão deste problema não tem precedentes; constata que tal poderá criar uma situação em que as infraestruturas de recolha e tratamento de dados em larga escala poderão ser utilizadas de forma abusiva em caso de mudança de regime político;

15. Observa que 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 ataques de intrusos bem equipados («ausência de segurança informática a 100 %»); constata que, com vista a alcançar a máxima segurança informática, os europeus precisam de estar dispostos a dedicar recursos suficientes, tanto humanos como financeiros, à preservação da independência e da autossuficiência da Europa no domínio informático;

16. Rejeita determinantemente a noção de que todas as questões relacionadas com os programas de vigilância em larga escala são puramente questões de segurança nacional e, por conseguinte, apenas da competência dos Estados-Membros; reafirma que os Estados-Membros devem respeitar plenamente o direito da UE e a CEDH, atuando simultaneamente para assegurar a sua segurança nacional; 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»[(41)]; recorda, além 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 da UE;

17. Louva 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 Estados Unidos e de deputados dos parlamentos nacionais;

18. 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;

19. Tenciona pedir fortes compromissos políticos à nova Comissão, a designar após as eleições europeias de maio de 2014, para executar as propostas e as recomendações deste inquérito;

Recomendações

20. Insta as autoridades dos Estados Unidos e os Estados-Membros da UE, nos casos em tal não se verifique já, a proibirem as atividades de vigilância em larga escala;

21. Insta os Estados-Membros da UE, e em particular os que participam nos chamados programas «9 Eyes» e «14 Eyes»[(42)], a avaliarem amplamente e, se necessário, a reverem a sua legislação nacional e as práticas que regem as atividades dos serviços de informação, por forma a assegurar que estejam sujeitos a supervisão parlamentar e judicial e ao controlo público, que respeitem os princípios da legalidade, necessidade, proporcionalidade, garantias processuais, notificação do utente e transparência, tendo também como base as compilações de boas práticas das Nações Unidas e as recomendações da Comissão de Veneza, que estejam em conformidade com as normas da Convenção Europeia dos Direitos do Homem e que cumpram as obrigações em matéria de direitos fundamentais dos Estados-Membros, nomeadamente no que diz respeito à proteção de dados, privacidade e presunção da inocência;

22. Apela a todos os Estados-Membros da UE, e, em particular o Reino Unido, a França, a Alemanha, a Suécia, os Países Baixos e a Polónia, à luz da sua Resolução de 4 de julho de 2013 e das audições no âmbito do inquérito, para que assegurem que os seus atuais ou futuros quadros legislativos e mecanismos de supervisão aplicáveis às atividades dos serviços de informação estejam em conformidade com as normas da Convenção Europeia dos Direitos do Homem e a legislação da União Europeia em matéria de proteção de dados; exorta estes Estados-Membros a clarificarem as alegações de atividades de vigilância em larga escala, incluindo a vigilância indiscriminada e generalizada de telecomunicações transfronteiriças, a vigilância aleatória em comunicações por cabo, os potenciais acordos entre serviços de informação e empresas de telecomunicações no que diz respeito ao acesso e ao intercâmbio de dados pessoais e acesso a cabos transatlânticos, pessoal e equipamento de informação dos Estados Unidos no território da UE sem supervisão das operações de vigilância, e respetiva compatibilidade com a legislação da UE; convida os parlamentos nacionais desses países a intensificarem a cooperação dos seus órgãos de supervisão dos serviços de informação a nível europeu;

23. Exorta o Reino Unido, em especial, dadas as amplas informações vindas a lume nos meios de comunicação social relativas à vigilância em larga escala pelos serviços de informação GCHQ, a rever o seu 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;

24. Toma nota da revisão da lei neerlandesa relativa à informação e segurança, de 2002 (relatório da «Comissão Dessens» de 2 de dezembro de 2013); apoia as recomendações da comissão de revisão que visam reforçar a transparência e o controlo e a supervisão dos serviços de informação neerlandeses; insta os Países Baixos a absterem-se de alargar os poderes dos serviços de informação de tal forma que a vigilância indiscriminada e em larga escala possa também ser efetuada em comunicações por cabo de cidadãos inocentes, especialmente tendo em conta o facto de um dos maiores nós de interconexão da Internet do mundo se encontrar em Amesterdão (AMS-IX); insta à prudência na definição do mandato e das capacidades da nova Ciberunidade Conjunta Sigint, bem como no que diz respeito à presença e operacionalidade de pessoal de informação dos Estados Unidos em território neerlandês;

25. Insta os Estados-Membros, incluindo quando representados pelas suas agências de informação, 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;

26. Exorta ao termo da interceção e do tratamento em larga escala de imagens «webcam» por qualquer serviço secreto; insta os Estados-Membros a procederem a uma investigação cabal sobre a questão de saber como e em que medida os respetivos secretos estiveram eventualmente envolvidos na recolha e no tratamento de imagens obtidas por «webcam» e a suprimirem todas as imagens registadas através desses programas de vigilância em larga escala;

27. Exorta os Estados-Membros a cumprirem imediatamente a sua obrigação positiva decorrente da Convenção Europeia dos Direitos do Homem de proteger os seus cidadãos da vigilância realizada

por países terceiros ou pelos seus próprios serviços de informação que seja contrária aos seus requisitos da mesma constantes, incluindo quando o objetivo é o de salvaguardar a segurança nacional, bem como a garantirem que o Estado de direito não seja enfraquecido em resultado da aplicação extraterritorial da legislação de um país terceiro;

28. 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»;

29. Insta os Estados-Membros a tomarem, sem demora, medidas adequadas, 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 a utilizarem todas as medidas internacionais disponíveis para defenderem os direitos fundamentais dos cidadãos da UE, nomeadamente desencadeando o procedimento de reclamação entre Estados previsto no artigo 41.º do Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP);

30. Solicita aos Estados-Membros que prevejam mecanismos efetivos por força dos quais as pessoas responsáveis por programas de vigilância (em larga escala) não consentâneos com o Estado de direito e os direitos fundamentais dos cidadãos respondam por este abuso de poder;

31. Apela aos Estados Unidos 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, de colocar os direitos dos cidadãos da UE em pé de igualdade com os direitos dos cidadãos dos Estados Unidos, e de assinar o Protocolo Facultativo que permite a apresentação de reclamações por indivíduos ao abrigo do PIDCP;

32. Saúda, a este respeito, as declarações proferidas e a «Diretiva Política Presidencial» promulgada pelo presidente dos Estados Unidos, Barack Obama, em 17 de janeiro de 2014, como um avanço para limitar a autorização do uso da vigilância e do tratamento de dados para efeitos de segurança nacional e um avanço para a igualdade de tratamento de todas as informações pessoais dos indivíduos, independentemente da nacionalidade ou residência, pela comunidade de informação dos Estados Unidos; aguarda, contudo, no contexto da relação UE-EUA, avanços mais específicos que reforçarão, essencialmente, a confiança nas transferências de dados transatlânticas e fornecerão garantias vinculativas para os direitos de privacidade que os cidadãos da UE podem fazer valer, como definido em pormenor no presente relatório;

33. Expressa a sua séria preocupação relativamente ao trabalho no seio do Comité de Convenção sobre a cibercriminalidade do Conselho da Europa em relação à interpretação do artigo 32.º da Convenção sobre cibercriminalidade de 23 de novembro de 2001 (Convenção de Budapeste) sobre o acesso transfronteiras a dados armazenados em computador, com consentimento ou quando disponíveis ao público, e opõe-se à conclusão de qualquer protocolo ou orientações adicionais que pretendam alargar o âmbito desta disposição para além do atual regime estabelecido por esta Convenção, que já constitui uma grande exceção ao princípio da territorialidade, porquanto poderia resultar num acesso à distância ilimitado por parte das forças de segurança aos servidores e sistemas informáticos localizados noutras jurisdições, sem recurso aos acordos AJM e aos outros instrumentos de cooperação judicial criados para garantir os direitos individuais fundamentais, incluindo a proteção de dados e das garantias processuais, nomeadamente a Convenção n.º 108 do Conselho da Europa;

34. 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;

35. Exorta a Agência dos Direitos Fundamentais a realizar uma investigação aprofundada sobre a proteção dos direitos fundamentais no contexto da vigilância, e nomeadamente sobre a atual

situação jurídica dos cidadãos da UE no que respeita às vias de recurso disponíveis em relação a essas práticas;

Transferências internacionais de dados
Quadro jurídico dos Estados Unidos em matéria de proteção de dados e «porto seguro»

36. 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 Estados Unidos são empresas que declararam a sua adesão ao princípio de «porto seguro», e que o «porto seguro» é o instrumento jurídico utilizado para a transferência de dados pessoais da UE para os EUA (por exemplo, Google, Microsoft, Yahoo!, Facebook, Apple e LinkedIn); manifesta preocupação relativamente ao facto de estas organizações não terem encriptado as informações e comunicações que são transferidas entre os seus centros de dados, permitindo que estas sejam intercetadas pelos serviços de informação; congratula-se com as declarações subsequentes de algumas empresas dos Estados Unidos de que acelerarão os planos para aplicar a encriptação dos fluxos de dados entre os seus centros de dados globais;

37. Considera que o acesso em larga escala pelas agências de informação dos Estados Unidos a dados pessoais da UE tratados segundo o princípio do «porto seguro» não cumpre os critérios de derrogação ao abrigo da «segurança nacional»;

38. 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, desde que estes instrumentos prevejam garantias e proteções específicas e não sejam contornados recorrendo a outros quadros jurídicos;

39. Considera que a Comissão não conseguiu agir de forma a atenuar as conhecidas lacunas da atual execução do «porto seguro»;

40. Exorta a Comissão a apresentar medidas que prevejam a suspensão imediata da Decisão 2000/520/CE da Comissão, que estabelecia a adequação do nível de proteção assegurado pelos princípios de «porto seguro» e pelas FAQ conexas emitidas pelo Departamento de Comércio dos EUA; solicita, por conseguinte, às autoridades dos Estados Unidos que apresentem uma proposta relativa a um novo quadro para as transferências de dados pessoais da UE para os EUA, que cumpra os requisitos da legislação de dados em matéria de proteção dos dados e preveja o nível adequado de proteção requerido;

41. 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 salvaguardas necessárias de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas;

42. Insta a Comissão a apresentar, até dezembro de 2014, uma avaliação exaustiva do quadro em matéria de proteção da vida privada dos Estados Unidos que cubra as atividades comerciais, de aplicação da lei e de informação, e recomendações concretas baseadas na falta de uma lei geral em matéria de proteção de dados nos Estados Unidos; encoraja a Comissão a entabular conversações com a administração dos EUA, a fim de estabelecer um quadro jurídico que preveja um elevado nível de proteção das pessoas no que diz respeito à proteção dos seus dados pessoais quando transferidas para os EUA e de assegurar a equivalência de quadros em matéria de proteção da vida privada da UE e dos EUA;

Transferências para outros países terceiros acompanhadas de uma decisão de adequação

43. 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 nacionais adotadas nos termos das demais 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;

44. Recorda que a Diretiva 95/46/CE também prevê que a adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias ligadas à operação de transferência dos dados ou ao conjunto de tais operações; 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; recorda que a Diretiva 95/46/CE habilita ainda a Comissão a declarar que um país terceiro não assegura um nível adequado de proteção;

45. 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;

46. Insta a Comissão e os Estados-Membros a avaliarem, sem mais delongas, se o nível adequado de proteção propiciado pelo *Privacy Act* da Nova Zelândia e da lei canadiana sobre dados pessoais e documentos eletrónicos, segundo declarado nas decisões 2013/65/UE e 2002/2/CE da Comissão, foi afetado pelo envolvimento das agências de informação nacionais desses países na vigilância em larga escala dos cidadãos da UE e, se necessário, a tomarem medidas adequadas para suspender ou revogar as decisões de adequação; insta igualmente a Comissão a avaliar a situação de outros países que receberam um nível de adequação; espera que a Comissão comunique ao Parlamento as suas conclusões relativamente aos países supramencionados o mais tardar até dezembro de 2014;

Transferências baseadas em cláusulas contratuais e noutros instrumentos

47. Recorda que as autoridades nacionais de proteção de dados indicaram que nem as cláusulas contratuais-tipo nem as normas empresariais vinculativas foram formuladas 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 devido a interesse legítimo numa sociedade democrática e sempre que tal seja necessário e proporcional;

48. 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 seja provável que a legislação a que o destinatário de dados está sujeito lhe impõe requisitos que ultrapassam as restrições estritamente necessárias, adequadas e proporcionadas numa sociedade democrática e que possam ter um efeito adverso nas garantias previstas na legislação em matéria de proteção de dados aplicável e nas cláusulas contratuais-tipo, ou nos casos em que a continuação da transferência dos dados possa criar um risco de danos graves para os titulares dos dados;

49. 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 vida privada, dos direitos fundamentais e das liberdades dos indivíduos, tendo especialmente em conta a legislação de países terceiros em matéria de 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;

50. Exorta a Comissão a examinar, sem demora, 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

51. 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 Estados Unidos 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; considera que tal avaliação não deve apenas considerar as declarações oficiais dos Estados Unidos como uma base suficiente para análise, mas basear-se também em avaliações específicas da UE; entende que 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; solicita igualmente ao Conselho e à Comissão que avaliem os acordos bilaterais entre os Estados-Membros e os Estados Unidos, a fim de zelar pela coerência entre tais acordos e os que a UE mantém ou decida vir a celebrar com os EUA;

Auxílio mútuo na UE em matéria penal

52. 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

53. Considera que as informações fornecidas pela Comissão Europeia e pelo Tesouro dos Estados Unidos não esclarecem se as agências de informação norte-americanas têm acesso às mensagens financeiras 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;

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

55. Insta a Comissão a reagir às preocupações concitadas pelo facto de três dos principais sistemas informatizados de reserva utilizados pelas linhas aéreas em todo o mundo estarem baseados nos Estados Unidos e de os dados PNR serem gravados em sistemas de computação em nuvem em funcionamento em solo americano, ao abrigo do direito dos Estados Unidos, o que carece de adequada proteção de dados;

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

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

57. Solicita um reatamento imediato das negociações com os Estados Unidos sobre o «acordo-quadro», que deverá pôr os direitos dos cidadãos da UE em pé de igualdade com os direitos dos cidadãos dos Estados Unidos; salienta, além disso, que este acordo deve prever vias de recurso administrativo e judicial eficazes e exequíveis para todos os cidadãos da UE nos Estados Unidos sem qualquer discriminação;

58. 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 com os Estados Unidos, enquanto o «acordo global» não tiver entrado em vigor;

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

Reforma de proteção de dados

60. Insta a Presidência do Conselho e os Estados-Membros a acelerarem os seus trabalhos sobre o pacote relativo à proteção de dados, a fim de permitir a sua adoção em 2014, para que os cidadãos da UE possam beneficiar de um nível elevado de proteção num futuro muito próximo; salienta que o firme empenho e o pleno apoio por parte do Conselho constituem condições necessárias para demonstrar credibilidade e firmeza em relação a países terceiros;

61. 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; salienta que só adotará medidas adicionais de cooperação em matéria de aplicação da lei quando o Conselho tiver encetado negociações com o Parlamento e a Comissão sobre o pacote relativo à proteção dos dados;

62. Recorda que os conceitos da «vida privada desde a conceção» e de «parâmetros predefinidos de proteção da vida privada» reforçam a proteção dos dados e devem servir de linhas diretrizes a seguir no que diz respeito a todos os produtos, serviços e sistemas oferecidos pela Internet;

63. Considera que o reforço da transparência e das normas de segurança aplicáveis à comunicação em linha e às telecomunicações constituem princípios necessários para melhorar o regime de proteção dos dados; solicita, por isso, à Comissão que apresente uma proposta legislativa sobre as condições gerais normalizadas relativas às comunicações em linha e às telecomunicações e que incumba um órgão de supervisão de verificar o cumprimento das condições gerais;

Computação em nuvem

64. Observa que a confiança na computação em nuvem e nos prestadores de serviços de computação em nuvem dos Estados Unidos foi prejudicada pelas práticas supramencionadas; enfatiza, por conseguinte, o desenvolvimento de sistemas de computação em nuvem e de soluções informáticas 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;

65. Exorta todos os órgãos públicos na União a não utilizarem os serviços em nuvem que possam estar sujeitos à legislação de países terceiros;

66. Reitera a sua grande preocupações 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 ou que utilizem servidores de armazenagem localizados em países terceiros e relativamente ao acesso remoto direto a dados pessoais e informação tratados por autoridades policiais e serviços de informação de países terceiros;

67. Deplora 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;

68. Insta a Comissão e os Estados-Membros a acelerarem os trabalhos com vista à criação da parceria europeia para a computação em nuvem, integrando plenamente a sociedade civil e a comunidade técnica, tal como a Task Force de Engenharia da Internet (IETF), e incluindo aspetos relativos à proteção de dados;

69. Exorta a Comissão, ao negociar acordos internacionais que impliquem o tratamento de dados pessoais, a prestar especial atenção aos riscos e desafios que a computação em nuvem representa para os direitos fundamentais, em especial - mas não exclusivamente - o direito à vida privada e à proteção dos dados pessoais, conforme estabelecido nos artigos 7.° e 8.° da Carta dos Direitos Fundamentais da União Europeia; insta ainda a Comissão a tomar nota das regras internas do parceiro de negociação relativas ao acesso das autoridades policiais e das agências de informação aos dados pessoais tratados através de serviços de computação em nuvem, em particular exigindo que o acesso só possa ser concedido no respeito pleno das devidas garantias jurídicas e se assentar numa base jurídica inequívoca, bem como impondo a obrigação de especificar as condições exatas do acesso, o motivo para dispor desse acesso, as medidas de segurança postas em prática quando da transmissão dos dados e os direitos dos indivíduos, bem como as regras aplicáveis à supervisão e a um mecanismo eficaz de recurso;

70. Salienta que todas as empresas que prestam serviços na UE devem, sem exceção, cumprir a legislação da UE e são responsáveis por quaisquer violações, e sublinha a importância da existência de sanções administrativas efetivas, proporcionadas e dissuasivas que podem ser impostas aos prestadores de serviços de «computação em nuvem» que não cumpram as normas de proteção de dados da UE;

71. Exorta a Comissão e as autoridades competentes nos Estados-Membros a avaliarem em que medida as normas da UE relativas à vida privada e à proteção de dados foram violadas devido à cooperação entre as entidades legais da UE e os serviços secretos ou à aceitação de mandados judiciais oriundos de autoridades de países terceiros, solicitando, em contradição com a legislação da UE em matéria de proteção de dados, dados pessoais de cidadãos da UE;

72. Exorta as empresas prestadoras de novos serviços, que recorram a «megadados», e de novas aplicações, como a «internet das coisas», a integrarem, já na fase de desenvolvimento, medidas relativas à proteção de dados, a fim de manter um nível de confiança elevado entre os cidadãos;

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

73. Reconhece que a UE e os Estados Unidos estão a efetuar negociações relativas a Parceria Transatlântica de Comércio e Investimento, de grande importância estratégica para um maior crescimento económico;

74. Enfatiza convictamente, dada a importância da economia digital na relação e para efeitos de restabelecimento da confiança EU-EUA, que, na falta de uma solução prévia adequada relativamente aos direitos à privacidade dos dados dos cidadãos da UE, incluindo o recurso administrativo e judicial, a aprovação pelo Parlamento do Acordo TTIP final está comprometida enquanto não cessarem por completo as atividades de vigilância em larga escala, bem como a interceção de comunicações no seio das instituições e das representações diplomáticas da UE; sublinha que o Parlamento pode apenas dar a sua aprovação ao Acordo TTIP final se este acordo respeitar na íntegra, nomeadamente os direitos fundamentais reconhecidos pela Carta da UE, e se a proteção da vida privada dos indivíduos em relação ao tratamento e à divulgação de dados pessoais continuar a ser regida pelo artigo XIV do GATS; salienta que a legislação da UE relativa à proteção de dados não pode ser considerada «arbitrária ou uma discriminação injustificável» na aplicação do artigo XIV do GATS;

Controlo democrático dos serviços de informação

75. Salienta que, apesar de o controlo das atividades dos serviços de informação se dever basear na legitimidade democrática (sólido 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 Estados Unidos demonstram uma falta notável de ambos, em particular das capacidades técnicas;

76. 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 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, incluindo o direito a efetuar visitas no local, para controlar eficazmente os serviços de informação;

77. Exorta à criação de um grupo de deputados e de peritos para examinar, de forma transparente e em colaboração com os parlamentos nacionais, recomendações para reforçar o controlo democrático, incluindo o controlo parlamentar, dos serviços de informação e a cooperação a nível do controlo na UE, nomeadamente no que respeita à sua dimensão transfronteiriça; considera que o grupo deverá examinar, em particular, a possibilidade de definir 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 organismos internacionais (Nações Unidas, Conselho da Europa), incluindo a questão dos organismos de supervisão considerados terceiros ao abrigo da «regra dos terceiros» ou do princípio do «controlo pela entidade de origem», em relação ao controlo e à responsabilização dos serviços de informação de países terceiros, critérios sobre o reforço da transparência assentes no princípio geral de acesso à informação e nos chamados «Princípios de Tschwane»[(43)], bem como nos princípios relativos aos limites aplicáveis à duração e ao âmbito de qualquer vigilância garantindo que sejam proporcionais aos objetivos;

78. Exorta este grupo a preparar um relatório destinado a uma conferência a realizar pelo Parlamento, em conjunto como os organismos nacionais de controlo, quer sejam de cariz parlamentar ou independente, até ao início de 2015, e a contribuir para a preparação da referida conferência;

79. 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;

80. 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);

81. Exorta a AR/VP a prestar regularmente contas das atividades do Centro da UE para a Análise de Informações (IntCen), que é parte integrante do Serviço Europeu para a Ação Externa, aos órgãos responsáveis do Parlamento, nomeadamente no que se refere à plena conformidade com os direitos humanos e as regras aplicáveis na UE em matéria de privacidade dos dados, permitindo um reforço da supervisão, por parte do Parlamento, da dimensão externa das políticas da UE; insta a Comissão e a AR/VP a apresentarem uma proposta de base jurídica para as atividades do IntCen, caso sejam consideradas operações ou futuras competências no âmbito de mecanismos próprios de recolha de informações e de dados que possam ter impacto na estratégia de segurança interna da UE;

82. Insta a Comissão a apresentar, até dezembro de 2014, uma proposta relativa a 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;

83. Recorda as disposições do Acordo Interinstitucional entre o Parlamento 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 melhorar o controlo a nível da UE;

Agências da UE

84. 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; considera que a Europol não deve transmitir qualquer informação ou dado obtido em violação de direitos fundamentais que deveriam estar protegidos pela Carta dos Direitos Fundamentais;

85. Insta a Europol a utilizar plenamente o seu mandato para solicitar às autoridades competentes dos Estados-Membros que deem início a inquéritos penais, no que diz respeito a ciberataques e a violações informáticas graves com potencial impacto transfronteiriço; considera que o mandato da Europol deveria ser reforçado para que possa dar início à sua própria investigação, na sequência de suspeita de um ataque malicioso à rede e aos sistemas de informação de dois ou mais Estados-Membros ou organismos da União[(44)]; insta a Comissão a supervisionar as atividades do Centro Europeu da Cibercriminalidade (EC3) e a apresentar, se necessário, uma proposta relativa a um quadro global para reforçar as suas competências;

Liberdade de expressão

86. 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;

87. Toma nota da detenção de David Miranda e da apreensão do material que se encontrava na sua posse pelas autoridades do Reino Unido ao abrigo do Apêndice 7 do *Terrorism Act* 2000 (e também o pedido ao jornal «The Guardian» para que destruísse ou entregasse o material) e expressa a sua preocupação pelo facto de tal constituir uma eventual violação grave do direito à liberdade de expressão e de imprensa consagrado no artigo 10.º da CEDH e no artigo 11.º da Carta da UE e de essa legislação destinada a combater o terrorismo poder ser utilizada abusivamente em tais casos;

88. Chama a atenção para a situação de denunciantes e dos seus apoiantes, incluindo os jornalistas na sequência das suas revelações; exorta a Comissão a conduzir uma análise sobre a questão de saber se uma futura proposta legislativa que estabeleça um programa europeu eficaz e abrangente para a proteção dos autores de denúncias, como já requerido na resolução do Parlamento de 23 de outubro de 2013, deveria também incluir outros domínios da competência da União, com particular atenção para a complexidade daa atividades de denúncia no domínio das informações de segurança; exorta os Estados-Membros a examinarem aprofundadamente a possibilidade de concederem aos denunciantes proteção internacional contra processos penais;

89. Exorta os Estados-Membros a assegurarem que a sua legislação, nomeadamente em matéria de segurança nacional, constitua uma alternativa segura ao silêncio por divulgar ou comunicar disfuncionamentos, incluindo corrupção, infrações penais, violação de obrigações jurídicas, erros judiciais e abuso de autoridade, que também está de acordo com as disposições dos diferentes instrumentos internacionais (Nações Unidas e Conselho da Europa) contra a corrupção, os princípios estabelecidos na Resolução PACE 1729 (2010), os princípios Tshwane, etc.;

Segurança informática na UE

90. 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 e software malicioso; 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; 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; sublinha que o reforço da capacidade e da segurança informática da UE também reduz a vulnerabilidade da UE em relação aos ciberataques graves provenientes de grandes organizações criminosas ou grupos terroristas;

91. 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, enquanto medida prioritária estratégica, uma capacidade de recursos informáticos fundamentais forte e autónoma; salienta que, por forma a criar confiança, essa capacidade de recursos informáticos europeia deve assentar, na medida do possível, em normas abertas e em software e, se possível, hardware de fonte aberta, de modo a que todo o processo possa ser revisto por toda e qualquer parte interessada, da conceção do processador até ao nível de aplicação; salienta que, no intuito de recuperar a competitividade no setor estratégico dos serviços informáticos, é necessário um novo pacto digital, bem como atividades conjuntas e de grande escala por parte das instituições europeias, dos governos dos Estados-Membros, da indústria e da sociedade civil; 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 de vida privada da UE num requisito de base para os contratos públicos de bens e serviços de informática; insta, por conseguinte, a Comissão a proceder à revisão das atuais práticas em matéria de contratos públicos, no que respeita ao tratamento de dados, a fim de ponderar circunscrever os contratos públicos às empresas certificadas, e eventualmente a empresas da UE, caso estejam envolvidos interesses de segurança ou interesses vitais;

92. Condena com veemência o facto de os serviços de informação terem procurado reduzir as normas de segurança informática e instalado «falhas de segurança» (backdoors) num vasto conjunto de sistemas informáticos; solicita à Comissão que apresente uma proposta legislativa no intuito de proibir a utilização de «falhas de segurança» (backdoors) por parte das autoridades responsáveis pela aplicação da lei; recomenda, por conseguinte, a utilização de software de código fonte aberto em todos as situações em que a segurança informática constitui uma preocupação;

93. Insta todos os Estados-Membros, a Comissão, o Conselho e o Conselho Europeu a darem o maior apoio possível, incluindo no domínio da investigação e desenvolvimento, ao reforço das capacidades de inovação e tecnologia europeias em termos de ferramentas, empresas e prestadores de serviços de informática (hardware, software, serviços e redes), nomeadamente para efeitos de cibersegurança e de capacidades de encriptação e criptografia; apela a todas as instituições competentes da UE e aos Estados-Membros para que invistam em tecnologias europeias locais e independentes e para que reforcem e desenvolvam maciçamente capacidades de deteção;

94. Insta a Comissão, os organismos de normalização e a ENISA a desenvolverem, até dezembro 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 e a integridade de todos os sistemas informáticos da UE; considera que estas normas poderiam tornar-se a referência para novas normas mundiais e 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; exprime o seu apoio às recentes decisões da Task Force de Engenharia da Internet (IETF), que preveem a inclusão dos governos nos modelos de ameaças à segurança na Internet;

95. Salienta que os reguladores de telecomunicações nacionais e da UE, e, em alguns casos, as empresas de telecomunicações, 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 de extremo a extremo das comunicações;

96. 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; sublinha a necessidade de uma segurança informática mais forte e de sistemas informáticos mais resistentes;

97. 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);

98. Apela à Comissão, no contexto do próximo Programa de Trabalho do Programa Horizonte 2020, para que dedique mais recursos ao impulsionamento da investigação, desenvolvimento, inovação e formação na Europa no domínio da informática, em particular no domínio das tecnologias e infraestruturas de reforço da privacidade, da criptologia, da computação segura, das melhores soluções em matéria de segurança, incluindo de fonte aberta, e outros serviços da sociedade da informação, e para que fomente o mercado interno de software e hardware europeus, e promova instrumentos de encriptação no domínio da comunicação e das infraestruturas de comunicação, nomeadamente através do desenvolvimento de uma estratégia global da UE para a indústria informática; considera que as pequenas e médias empresas desempenham um papel importante no domínio da investigação; salienta que não devem ser consagrados quaisquer recursos financeiros da UE a projetos que tenham por fim exclusivo o desenvolvimento de instrumentos para obter acesso ilícito a sistemas informáticos;

99. Solicita à Comissão que defina as atuais responsabilidades e que reveja, o mais tardar até dezembro de 2014, a necessidade de um mandato mais amplo, de uma melhor coordenação e/ou de recursos e capacidades técnicas adicionais para a ENISA, o centro de cibercriminalidade da Europol e outros centros da União que disponham de conhecimentos especializados, a CERT-UE e a AEPD, a fim de lhes permitir desempenhar um papel-chave na segurança dos sistemas de comunicação europeus e ser mais eficazes na prevenção e 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; insta, em particular, a Comissão a ponderar o reforço do papel da ENISA na defesa dos sistemas internos no seio das instituições da UE e a estabelecer, no âmbito da estrutura da ENISA, uma equipa competente de resposta a situações de emergências (CERT) para a UE e os seus Estados-Membros;

100. Solicita à Comissão que avalie a necessidade suplementar de criar uma Academia de Informática da UE que reúna os melhores peritos europeus e internacionais independentes 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;

101. Insta os serviços competentes do secretariado do Parlamento Europeu, sob a responsabilidade do Presidente do Parlamento, a realizar, o mais tardar até junho de 2015, com um relatório intercalar o mais tardar até dezembro 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 do Parlamento; 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 de melhores práticas específicos em matéria de segurança/privacidade informática, incluindo a

possibilidade de um requisito de software de fonte aberta como condição de compra, ou o requisito da participação no concurso de empresas europeias de confiança, sempre que estejam em causa domínios sensíveis, relacionados com a segurança;

– a lista das empresas com contratos com o Parlamento nos domínios da informática e das telecomunicações, tendo em conta qualquer informação revelada sobre a sua colaboração com serviços de informação (como as revelações sobre os contratos da NSA com uma empresa como a RSA, cujos produtos o Parlamento utiliza para, presumivelmente, proteger o acesso à distância aos seus dados pelos seus membros e pessoal), incluindo a exequibilidade de os mesmos serviços serem providenciados por empresas, de preferência europeias;
– a fiabilidade e a resistência de software, especialmente de sistemas comerciais prontos a usar, 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, tendo também em conta as normas internacionais pertinentes, os princípios de gestão de risco que correspondam às melhores práticas e a adesão às normas da UE de Segurança das Redes e da Informação em matéria de violações da segurança;
– a utilização de mais sistemas de fonte aberta;
– os passos e as medidas a tomar para dar resposta ao 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 e dos sistemas informáticos utilizados no Parlamento;
– a utilização e localização de servidores e centros de informática dos sistemas informáticos do Parlamento 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 de serviços de computação e de armazenagem em nuvem pelo Parlamento, incluindo o tipo de dados armazenados em nuvem, a forma como os conteúdos e o acesso aos mesmos são protegidos e a localização do servidor em nuvem, clarificando o regime jurídico de proteção de dados e de informações de segurança aplicável, bem como a avaliação das possibilidades de apenas usar servidores em nuvem que estejam localizados em território da UE;
– 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 assinaturas eletrónicas no correio eletrónico;
– um plano para a utilização da norma de encriptação predefinida, como o *GNU Privacy Guard*, para o correio eletrónico, que permitiria, ao mesmo tempo, a utilização de assinaturas digitais;
– a possibilidade de criar um serviço seguro de mensagens instantâneas no Parlamento que permita comunicações seguras, em que o servidor apenas teria acesso a conteúdo encriptado;

102. Insta todas as instituições e agências da UE a realizarem, em cooperação com a ENISA, a Europol e as CERT, um exercício semelhante, o mais tardar até junho de 2015, com um relatório intercalar 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;

103. 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;

104. Considera que os sistemas informáticos em 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, como o UE-ESTA, deveriam ser desenvolvidos e operados de forma a garantir que os dados não sejam comprometidos na sequência de pedidos das autoridades de países terceiros; solicita à eu-LISA que comunique ao Parlamento informações sobre a fiabilidade dos sistemas em vigor até ao final de 2014;

105. Insta a Comissão e o SEAE a tomarem medidas a nível internacional, em particular com a ONU e em cooperação com parceiros interessados, 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, evitando, simultaneamente, facilitar o controlo e a censura estatais ou a «balcanização» e fragmentação da Internet;

106. Apela à UE para que assuma a liderança na remodelação da arquitetura e da governação da Internet, a fim de fazer face aos riscos relacionados com os 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 o reencaminhamento do tráfego na Internet ou a plena encriptação de extremo a extremo de todo o tráfego na Internet, de modo a evitar os atuais riscos associados a 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 vida privada;

107. Apela à promoção

- de motores de pesquisa e redes sociais da UE como um passo significativo para a independência informática da UE;
- de fornecedores de serviços informáticos europeus;
- da encriptação da comunicação em geral, incluindo do correio eletrónico e das comunicações por SMS;
- dos elementos informáticos europeus fundamentais, nomeadamente das soluções relativas aos sistemas operativos cliente-servidor, recorrendo a normas de fonte aberta e desenvolvendo elementos para ligação à rede, como routers;

108. Solicita à Comissão que apresente uma proposta legislativa para um sistema de rota da UE, incluindo um tratamento a nível da UE do registo dos pormenores de chamadas (CDR), que constituirá uma subestrutura da atual internet e não ultrapassará as fronteiras da UE; observa que todos os dados sobre o trajeto e todos os CDR devem ser tratados em conformidade com o quadro legislativo da UE;

109. 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 desenvolverem uma cultura de segurança e 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 encriptação e da computação em nuvem segura, fazendo pleno uso da plataforma de informação de interesse público prevista na Diretiva Serviço Universal;

110. Insta a Comissão a apresentar, até dezembro de 2014, propostas legislativas que incentivem os fabricantes de software e hardware a introduzirem uma maior segurança e privacidade, através de funcionalidades desde a conceção e predefinidas, nos seus produtos, nomeadamente mercê da introdução de desincentivos à recolha indevida e desproporcionada de dados pessoais em massa e da responsabilidade jurídica da parte dos fabricantes em relação a vulnerabilidades conhecidas não corrigidas, produtos defeituosos ou não seguros ou a instalação de «falhas de segurança» secretas, que permitam o acesso não autorizado a dados e respetivo tratamento; insta a Comissão a, a este respeito, avaliar as possibilidades de estabelecer um esquema de certificação e de validação para o hardware informático, incluindo métodos de ensaio a nível da UE, a fim de garantir a integridade e a segurança dos produtos;

Restabelecer a confiança

111. Acredita que o inquérito demonstrou, para além da necessidade de uma alteração do quadro legislativo, a necessidade de os Estados Unidos restabelecerem a confiança com os seus parceiros na UE, uma vez que estão em causa sobretudo as atividades das agências de informação norte-americanas;

112. 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 pelos direitos fundamentais, pela democracia e pelo Estado de direito, bem como à credibilidade das garantias democráticas, judiciais e parlamentares e à vigilância, numa sociedade cada vez mais digital;

Entre a UE e os EUA

113. 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;

114. 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 facto é ainda agravado pela ausência de possibilidades de recurso judicial e administrativo para os cidadãos da UE ao abrigo da legislação americana, particularmente em casos de atividades de vigilância para efeitos de informação;

115. Reconhece, à luz dos desafios globais que a UE e os EUA enfrentam, que a parceria transatlântica tem de ser reforçada e que é fundamental que a cooperação transatlântica na luta contra o terrorismo prossiga numa nova base de confiança, construída sobre um verdadeiro respeito comum pelo Estado de direito e sobre o repúdio de todas as práticas indiscriminadas de vigilância em larga escala; insiste, por conseguinte, que os EUA têm de tomar medidas claras para restabelecer a confiança e volta a enfatizar os valores básicos partilhados subjacentes à parceria;

116. Está preparado para encetar um 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, sejam abordados os direitos à vida privada e outros direitos dos cidadãos da UE, residentes ou outras pessoas protegidas pela legislação da UE, e outros direitos equivalentes à informação e à proteção da privacidade, incluindo o de recurso, nos tribunais norte-americanos através, por exemplo, da revisão do *Privacy Act* e do *Electronic Communications Privacy Act*, e da ratificação do primeiro protocolo opcional ao Pacto Internacional sobre Direitos Civis e Políticos (PIDCP), para que a atual discriminação não seja perpetuada;

117. Insiste em que sejam realizadas as reformas necessárias e dadas garantias eficazes aos europeus no sentido de garantir que o recurso à vigilância e ao tratamento de dados para efeitos de serviços de informação externos seja proporcionado, limitado por condições claramente especificadas, e esteja relacionado com suspeitas razoáveis ou causa provável de atividade terrorista; salienta que este objetivo deve estar sujeito a controlo judicial transparente;

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

119. Exorta a Comissão Europeia e a Administração dos EUA a, no contexto das negociações em curso sobre um acordo global UE-EUA relativo à transferência de dados para efeitos de aplicação da

lei, abordarem a questão dos direitos dos cidadãos da UE à informação e a recurso judicial, e a concluírem estas negociações, em consonância com o compromisso assumido na reunião ministerial «Justiça e Assuntos Internos» UE-EUA, de 18 de novembro de 2013, antes do verão de 2014;

120. 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 de 2001, reforçando assim a base jurídica partilhada pelos aliados transatlânticos;

121. 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

122. Entende, além disso, que o envolvimento e as atividades dos Estados-Membros da UE levaram a uma perda da confiança, nomeadamente entre Estados-Membros e entre os cidadãos e as respetivas autoridades nacionais; 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 e das práticas que visam pôr cobro às atividades de vigilância em larga escala e reforçar o sistema de controlo judicial e parlamentar serão capazes de restabelecer a confiança perdida; reafirma as dificuldades envolvidas no desenvolvimento de políticas de segurança europeias abrangentes face a tais atividades de vigilância em grande escala e salienta que o princípio da cooperação leal requer que os Estados-Membros se abstenham de realizar quaisquer atividades de informação no território de outro Estado-Membro;

123. Observa 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 respeitar plenamente os interesses e o quadro legislativo da UE na sua globalidade; considera este tipo de acordos bilaterais contraproducente e irrelevante, dada a necessidade de uma solução europeia para este problema; solicita ao Conselho que informe o Parlamento sobre os progressos alcançados pelos Estados-Membros relativamente a um acordo de não-espionagem mútua à escala da UE;

124. Considera que esses acordos não deverão violar os Tratados da União, principalmente o princípio da cooperação leal (nos termos do artigo 4.º, n.º 3, do TUE), nem comprometer as políticas da UE em geral e, mais especificamente, o mercado interno, a concorrência leal e o desenvolvimento económico, industrial e social; decide analisar qualquer acordo deste tipo sob o ponto de vista da sua compatibilidade com o Direito europeu e reserva-se o direito de ativar os procedimentos previstos nos Tratados, caso tais acordos se revelem contrários à coesão da União ou aos princípios fundamentais nos quais esta assenta;

125. Exorta os Estados-Membros a despenderem todos os esforços ao seu alcance para assegurar uma melhor cooperação visando fornecer garantias contra a espionagem, em colaboração com os organismos e agências da UE pertinentes, para a proteção dos cidadãos e as instituições da UE, as empresas europeias, a indústria da UE e as infraestruturas e redes de TI, bem como a investigação europeia; considera que a participação ativa das partes interessadas da UE constitui uma condição prévia indispensável para assegurar um intercâmbio de informações eficaz; chama a atenção para o facto de as ameaças de segurança se terem tornado mais internacionais, difusas e complexas, obrigando a um reforço da cooperação europeia; está convencido de que esta evolução deve estar mais bem espelhada nos Tratados, solicitando por isso que estes sejam revistos, de molde a reforçar a noção de cooperação leal entre os Estados-Membros e a União, no que toca ao objetivo de instaurar um espaço de segurança, e a evitar a espionagem entre Estados-Membros no seio da União;

126. Considera absolutamente necessária a existência, em todas as instituições e delegações pertinentes da UE, de estruturas de comunicação (correio eletrónico e telecomunicações, incluindo

linhas terrestres e telemóveis) e salas de reunião seguras contra escutas; solicita, por isso, a criação de um sistema interno da UE de correio eletrónico cifrado;

127. Solicita ao Conselho e à Comissão que aprovem imediatamente a proposta adotada pelo Parlamento Europeu, em 23 de maio de 2012, sobre um regulamento do Parlamento Europeu relativo às formas de exercício do direito de inquérito do Parlamento Europeu e que revoga a Decisão 95/167/CE, Euratom, CECA do Parlamento Europeu, do Conselho e da Comissão, apresentada com base no artigo 226.º do TFUE; solicita que o Tratado seja revisto de forma a alargar esses poderes de inquérito, para que cubram, sem restrições nem exceções, todos os domínios de competência ou de atividade da União, e incluam a possibilidade de proceder a interrogatórios sob juramento;

A nível internacional

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

129. 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 geral n.º 16 da Comissão dos Direitos do Homem 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»; insta os Estados-Membros a incluírem, em todo esse processo, um apelo à criação de uma agência internacional das Nações Unidas responsável por um controlo especial dos instrumentos de vigilância emergentes e pela regulamentação e investigação da sua utilização; solicita à Alta Representante/Vice-Presidente da Comissão e ao Serviço Europeu de Ação Externa que assumam uma postura pró-ativa;

130. 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 Terceira Comissão da Assembleia Geral da ONU (Comissão dos Direitos do Homem) em 27 de novembro de 2013, e tomando novas medidas de defesa do direito fundamental à vida privada e à proteção dos dados a nível internacional que, ao mesmo tempo, evitem facilitar o controlo e a censura estatais ou a fragmentação da Internet, como uma iniciativa tendente à adoção de um tratado internacional que proíba as atividades de vigilância em larga escala e à criação de uma agência encarregada da sua supervisão;

Plano de prioridades: um Habeas Corpus Digital Europeu - proteger os direitos fundamentais na era digital

131. 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; exorta a Comissão e demais instituições, órgãos, organismos e agências da UE referidos na presente resolução, em conformidade com o disposto no artigo 265.º do TFUE, a darem seguimento às recomendações e aos apelos constantes da presente resolução;

132. Decide lançar o plano «Um Habeas Corpus Digital Europeu - proteger os direitos fundamentais na era digital» que inclui as seguintes 8 ações, cuja realização supervisionará:

- Ação 1: adotar o pacote relativo à proteção de dados em 2014;
- Ação 2: celebrar o acordo global UE-EUA, garantindo o direito fundamental dos cidadãos à privacidade e à proteção dos dados e a existência de mecanismos adequados de recurso para os cidadãos da UE, inclusivamente em caso de transferências de dados da UE para os EUA para efeitos de aplicação da lei;
- Ação 3: suspender o dispositivo «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 possam 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: apreciar qualquer acordo, mecanismo ou intercâmbio com países terceiros que envolva dados pessoas, a fim de garantir que o direito à vida privada e à proteção dos dados pessoais não seja violado em consequência de atividades de vigilância e tomar as medidas de acompanhamento necessárias;
- Ação 6: proteger o Estado de direito e os direitos fundamentais dos cidadãos da UE (incluindo de ameaças à liberdade de imprensa), o direito do público a uma informação imparcial e à confidencialidade profissional (incluindo relações advogado-cliente), bem como garantir o reforço da proteção dos denunciantes;
- Ação 7: desenvolver uma estratégia europeia para uma maior independência informática (um «new deal digital» que inclua a afetação dos recursos apropriados a nível nacional e da UE) para promover a indústria informática e permitir às empresas europeias tirar partido da vantagem concorrencial da UE no plano da privacidade;
- Ação 8: desenvolver a UE como interveniente de referência na governação democrática e neutra da Internet;

133. Exorta as instituições da UE e os Estados-Membros a promoverem o «Habeas Corpus Digital Europeu», que protege os direitos fundamentais na era digital; compromete-se a agir como paladino dos direitos dos cidadãos da UE, cumprindo o seguinte calendário de acompanhamento da execução:

- Abril de 2014-Março de 2015: um grupo de acompanhamento baseado na equipa de inquérito da LIBE responsável pelo acompanhamento de novas revelações 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 que inclua o «Habeas Corpus Digital Europeu - proteger os direitos fundamentais na era digital» nas orientações a adotar ao abrigo do artigo 68.º do TFUE;
- Outono de 2014: um compromisso de que o «Habeas Corpus Digital Europeu - proteger os direitos fundamentais na era digital» e as recomendações conexas servirão de critérios de base para a aprovação da próxima Comissão;
- 2014: uma conferência que reúna peritos europeus de alto nível nos vários domínios que contribuem para a 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;
- 2014-2015: um grupo sobre Confiança/Dados/Direitos dos Cidadãos que, por convocação do Parlamento Europeu e do Congresso dos EUA, se reúna regularmente e, também, 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;

o
o o

134. 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;

135. Encarrega a sua Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos de abordar esta questão em plenário um ano após a aprovação da presente resolução; considera essencial avaliar o grau de cumprimento das recomendações aprovadas pelo Parlamento e analisar as razões, se for caso disso, que levaram a que não tivessem seguimento.

---

(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***

(3) ***http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf***

(4) http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx

(5) La Fédération Internationale des Ligues des Droits de l'Homme et La Ligue française pour la défense des droits de l'Homme et du Citoyen contre X; Tribunal de Grande Instance de Paris.

(6) Processos instaurados por Privacy International and Liberty perante o Investigatory Powers Tribunal.

(7) Pedido conjunto ao abrigo do artigo 34.º de Big Brother Watch, Open Rights Group, English Pen e Dr. Constanze Kurz (requerentes) contra o Reino Unido (requerido).

(8) JO C 197 de 12.7.2000, p. 1.

(9) JO C 121 de 24.4.2001, p. 152.

(10) ***http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf***

(11) JO L 204 de 4.8.2007, p. 18.

(12) JO L 215 de 11.8.2012, p. 5.

(13) SEC(2013) 0630, de 27 de novembro de 2013.

(14) Conclusões do Advogado-Geral Pedro Cruz Villalón, apresentadas em 12 de dezembro de 2013, no processo C-293/12.

(15) JO L 195 de 27.7.2010, p. 3.

(16) JO L 181 de 19.7.2003, p. 34.

(17) JO L 309 de 29.11.1996, p. 1.

(18) Documento 16987/2013 do Conselho.

(19) JO C 72 E de 21.3.2002, p. 221.

(20) JO C 16 E de 22.1.2001, p. 88.

(21) Textos aprovados, **P7_TA(2013)0203**.

(22) Textos aprovados, **P7_TA(2013)0322**.

(23) Textos aprovados, **P7_TA(2013)0444**.

(24) Textos aprovados, **P7_TA(2013)0449**.

(25) Textos aprovados, **P7_TA(2013)0535**.

(26) JO C 353 E de 3.12.2013, p. 156.

(27) Klayman et al. v Obama et al., Processo civil n.º 13-0851, 16 de dezembro de 2013.

(28) ACLU v. NSA n.º 06-CV-10204, 17 de agosto de 2006.

(29) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong/

(30) Acórdão no processo C-155/79, 18 de maio de 1982, AM & S Europe Limited contra a Comissão das Comunidades Europeias.

(31) *Vide*, nomeadamente, o acórdão de 28 de maio de 1991, nos processos apensos C-6/90 e C-9/90, Francovich e outros contra a República Italiana.

(32) JO L 28 de 30.1.2013, p. 12.

(33) JO L 2 de 4.1.2002, p. 13.

(34) A carta declara que o Governo dos Estados Unidos solicita e obtém dados financeiros recolhidos por vias regulamentares, de aplicação da lei, diplomáticas e de informação, bem como através de intercâmbios com parceiros estrangeiros, e que o Governo utiliza o Acordo TFTP para obter dados do SWIFT que não obtém de outras fontes.

(35) ***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***

(36) JO L 181 de 19.07.2003, p. 25.

(37) COM(2012) 0011 de 25.1.2012.

(38) COM(2012) 0010 de 25.1.2012.

(39) http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/pt/er/139197.pdf

(40) 1 BvR 518/02 de 4 de abril de 2006.

(41) Acórdão de 4 de junho de 2013 proferido no processo C-300/11, ZZ/Secretary of State for the Home Department.

(42) O programa «9 Eyes» engloba os EUA, o Reino Unido, o Canadá, a Austrália, a Nova Zelândia, a Dinamarca, a França, a Noruega e os Países Baixos; o programa «14 Eyes» inclui estes países e a Alemanha, a Bélgica, a Itália, a Espanha e a Suécia.

(43) «The Global Principles on National Security and the Right to Information» (Princípios mundiais relativos à segurança nacional e o direito à informação), junho de 2013.

(44) Posição do Parlamento Europeu, de 25 de fevereiro de 2014, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que cria a Agência da União Europeia para a Cooperação e a Formação Policial (Europol) (Textos Aprovados, **P7_TA(2014)0121**).